CYBERSPACE GOVERNANCE:
A STUDY OF RUSSIA'S APPROACH

Thesis submitted to Jawaharlal Nehru University

for the award of the degree of

DOCTOR OF PHILOSOPHY

SHOBHNA KUNWAR

Centre for Russian and Central Asian Studies

Jawaharlal Nehru University

New Delhi—110067

2017

JAWAHARLAL NEHRU UNIVERSITY

Centre for Russian and Central Asian Studies
School of International Studies
New Delhi-110067

Tel.: (O) +91-11-2670 4365
Fax: (+91) - 11-2674 1586, 2586
Email: crcasjnu@gmail.com

Date: 2017

DECLARATION

I declare that the thesis entitled **"Cyberspace Governance: A Study of Russia's Approach"** submitted by me for the award of the degree of DOCTOR OF **PHILOSOPHY** of **Jawaharlal Nehru University** is my own work. The thesis has not been submitted for any other degree of this University or any other university.

Shobha

SHOBHNA KUNWAR

CERTIFICATE

We recommend that this thesis be placed before the examiners for evaluation.

A. Upadhyay

Prof. Archana Upadhyay
(Chairperson, CRCAS)

A. Upadhyay

Prof. Archana Upadhyay
(Supervisor)

To the loved ones who have always stood by me and for Rocky and Rickina……

Contents

Acknowledgement

I am thankful to my supervisor, Prof. Archana Upadhyay who provided me support, critical inputs to finish this work. Several improvements came through after highly productive discussions with her. Writing this under her guidance has been a great learning experience.

I am also thankful to the faculty members who gave me several suggestions and inputs and encouraged me to keep improving the work. The office staff of the Centre for Russian and Central Asian Studies too has been very helpful. So, I extend my thanks to all office staff members.

The School of International Studies administration staff too has been prompt in providing help. Their timely action on matters of scholarship and field trip related processes were crucial to the research. I am thankful to them. I also thank JNU Library for giving me access to reading resources.

I am also thankful to Prof. Arthur Demchuk, Moscow State University, who helped in matters of my field trip and then in arranging interviews with scholars, to Prof. Eugenia Vanina, Institute of Oriental Studies, Moscow for guiding during the stay at Moscow, to Prof. Voldenkov, Department of Political Science, MSU and Alexandra Kulikova, PIR Center, Moscow for helping me gain new insights on my Ph.D. area.

Finally, I am thankful to my family and buddies for encouraging me to finish the work on time and with dedication.

Abbreviations

BBC	**British Broadcasting Corporation**
BRICS	**Brazil, Russia, India, China, South Africa**
CERT	**Computer Emergency Response Team**
CIA	**Central Intelligence Agency**
DDoS	**Distributed Denial of Service**
DARPA	**Defense Advanced Research Projects Agency**
DNS	**Domain Name System**
EFF	**Electronic Frontier Foundation**
FCC	**Federal Communication Commission**
FSB	**Federal’naya Sluzhba Bezopasnosti Rossiyskoy Federatsii**
GCHQ	**Government Communications Headquarters**
HTTP	**Hyper Text Transfer Protocol**
ICT	**Information and Communications Technology**
ICANN	**Internet Corporation for Assigned Names and Numbers**
IETF	**Internet Engineering Task Force**
IHL	**International Humanitarian Law**
IPv4	**Internet Protocol version 4**
IPv6	**Internet Protocol version 6**
ISP	**Internet Service Provider**
ITU	**International Telecommunication Union**
MPAA	**Motion Pictures Association of America**
NASA	**National Aeronautics and Space Administration**
NASDAQ	**National Association of Securities Dealers Automated Quotations**
NATO	**North Atlantic Treaty Organisation**
NSA	**National Security Agency**
OECD	**Organisation for Economic Cooperation and Development**
OPEC	**Organisation of Petroleum Exporting Countries**

PIPA	**Protect Intellectual Property Act**
PSYOPS	**Psychological Operations**
RT	**Russian Today**
SCO	**Shanghai Cooperation Organisation**
SOPA	**Stop Online Piracy Act**
SORM	**Sistema Operativno Rozysknih Meropriyatii**
TLD	**Top Level Domain**
TLF	**Technology Liberation Front**
TOI	**Times of India**
TRIPS	**Trade Related Aspects of Intellectual Property Rights**
UK	**United Kingdom**
USA	**United States of America**
WSIS	**World Summit on Information Society**
WSJ	**Wall Street Journal**
WTO	**World Trade Orgnanisation**
www	**World Wide Web**

Preface

Cyberspace has become important in our lives because it is almost everywhere. Its reach is wide and deep. Its impact is even bigger than its reach. It has changed the way people connect, talk, store and transfer information, share knowledge and have access to it. With this, new kind of security threats has come up too. Called by the umbrella term ‘cyber security threats’, these could be anything, from a breach into confidential file in the computer, snooping on conversation happening in a social media chat, hacking of the system, defacing of the website, DDoS attacks and penetration of a malware. These threats have compelled states to turn towards increasing their role in controlling cyberspace. This has come in the form of greater emphasis on cyber war more surveillance of citizens, regulations for access to content in Internet, laws for making claims, speech and expressing opinions online and emphasis on sovereignty over one’s information sphere. These have made governance of cyberspace a ground of contention. The contention is between basic models of governance: Multistakeholder approach and State led regulatory approach. The first one is an approach that allows participation of state and non-state stakeholders in cyberspace while the latter gives the leading space to state.

This work has discussed two issues in this context from perspective of Russia’s approach. First is ‘How does Russia’s position on regulating cyberspace transform the cyberspace governance?’. Second is ‘What are important factors that have influenced Russia’s regulation of cyberspace?’ Accordingly, the thesis puts to test two hypotheses. The first one is: Russian position on regulating cyberspace transforms the focus of cyberspace governance from ungovernability of cyberspace to cyber control by states. The second one is: Russia’s notion of regulation is informed by presence of online political activism and cyber crimes in Russia. The data for testing the hypotheses are discussed from Chapter 1 through Chapter 4, with the last Chapter 5 having the main findings. The first chapter titled *‘Introduction’* has put the research design of the thesis. This includes a review of the existing literature, main research questions, significance of this research for understanding cyberspace governance better, the framework or the assumption of the work which has been named as Invention-Innovation-

Practices-Spread-Entrenchment (IIPSE). This assumption is the framework through which the thesis seeks to understand the changes taking place due to innovations in cyberspace. The question of governance cannot be detached from the milieu of innovations and the practices they give rise to. Placing the understanding in this framework brings forth clarity of a how cyberspace governance is taking place and how is Russia placed in it.

The second chapter titled *'Cyberspace Governance: Issues and State Practices'* discusses some of the important cyberspace governance issues. These issues are part of the invention-innovation-practices-spread-entrenchment process. Inventions like Internet have been innovated many times through machine-human interface. Its new applications like social media, cyber crimes, cyber weapon are innovations that have given rise to practices like online political activism, cyber crimes, surveillance and so on. These have spread and states face challenges related to them. The third chapter titled *'Domestic Factors in Cyberspace Scenario in Russia'* has discussed cyberspace governance issues in Russia. The factors that have been highlighted are cyber crimes, online political activism, presence of American tech giants like Google and Facebook in Russia. The factors like cyber crimes and online political activism have received special attention as they form the independent variable in the second hypothesis. In cyber crimes, Russia's ecosystem of cyber crimes has been discussed. Online political activism has been discussed with reference to some related events in the last four years (approximately). This chapter has discussed how these two factors are increasingly becoming important in Russia. Fourth chapter titled *'Russian Approaches to Cyberspace Governance Issues'* has discussed three areas: Russia's surveillance system, the country's cyber diplomacy with two major players: USA and China, its multilateral efforts to articulate its position on cyberspace governance, control of Internet, and country's new laws or changes in existing laws to deal with threats posed by cyberspace governance and issues like online copyrights.

The last and fifth chapter *Conclusion* has put the main findings which are that analysis of the data corroborates both the hypotheses. In this, special mention has been made of the IIPSE process, the contentious nature of meaning of cyberspace, meaning of ungovernability and regulation. The IIPSE framework has been elaborately referred to with the help of issues mentioned in different chapters. The aim is to look at the conclusion from this perspective. Then the chapter has listed reasons for why the two hypotheses should be seen as getting strengthened in the light of some facts. There is also reference to areas that the thesis has left out and the ones that can be developed in another study. For the analysis, the study has relied on primary and secondary sources. Internet sources have been used and for a study on cyberspace governance, it has been helpful.

1.1 Introduction

Cyberspace has multiple meanings. In fact, there can be as many meanings of the term as there are scholars to study it. It has been seen as a technological marvel by the technology experts, that gives a virtual space. Political and social scientists see it as virtual space that weakens or strengthens state or social bonds. For several political activists, it means a space for uncensored freedom of thought and expression, while for some miscreants it may be a mere space for their unbridled activities that are sanctioned neither by laws nor by customs of the society. As opposed to all this, a view from the corporate sector sees it as a global commons whose uses need to remain open. The idea of balkanizing[1] its uses along lines of the borders between states appears appalling to their business mindsets. Quite a number of corporates also seems to find its meaning in the human-technology interface that can be regulated provided it makes some business sense. In this crowd of meanings, states of various political hues have their own sets of meanings. For a democratic country, it is a space that is free and should remain so. According to it, cyberspace may be better utilized if it is only put under a tab and is mildly regulated. As opposed to this, some autocratic regimes see cyberspace as an indiscipline horse that needs to be controlled and made to run in the ‘right and desired direction’. Therefore, many themes have developed in the literature which are discussed below.

1.2. Themes in Literature

1.2.1 Romantic/ Utopian and Dystopian Assumptions and Visions

There are some strongly held assumptions related to the division into Utopian and Dystopian visions of cyberspace. Several definitions have been given to the two types of thinkers, ideas or works. While sifting through the literature, the author discovers that there is a tendency to see any idea/work/ author as utopian or dystopian on the basis of whether the work or idea concerned considers cyberspace as some good space or force or some harbinger of doomsday. Even the

[1] Balkanize refers to the kind of splintering that the Balkan region suffered from after Soviet disintegration.

meanings of utopian are kept fixed in this. That is why terms like ‘cyber wild west’ or ‘unconquered territory’ are appropriated for utopian meanings of cyberspace. Even William Gibson’s rendering is brought under the romantic illusion in which cyberspace appears neither of this world nor of the other unknown. It is then quickly assumed that this or that work is cyber utopian on the basis of work’s perception of cyberspace as good or bad. It can be conceded that ‘visions’ do colour the meanings and perceptions but they are not present in tight compartments. There is instead some kind of spectrum where authors and their works vary in terms of beneficial effects or negative aspects that they see or wish to see. So, no work or author can be actually put in a closed box. This creates some space for skeptics or the middle ones who otherwise lose respect in any binary system in which virtues of clear stances are sought to be upheld.

The second important point about utopians or dystopians is that there has been a dominant tendency to ignore the importance of an author’s opinion on what cyberspace ‘should look like’. The ‘ought to be’ opinion may not be explicitly stated. Nevertheless, it is important to see this, as most authors take it as underlying assumption. For instance, when John Perry Barlow talks about declaring ‘freedom of cyberspace’ and castigates human run states for trying to interfere with the freedom of cyberspace, is he not being a utopian? He is utopian because it is implicit in his exhortations that he wishes to see cyberspace to be completely free from the hawk like grip of state. To concede a point, many do see Barlow as utopian, but a large spectrum remains untouched for extracting out the utopian or dystopian assumptions. This spectrum covers mainly skeptics who would not completely yield ground to either of the two extremes and their emphases on utopian and dystopian vary. The ideas presented by these authors or institutions are scattered in several disciplines, prominent being the political, sociological studies and psychology.

While forming stances on cyberspace, these studies have analysed and judged cyberspace nature on the basis of how cyber technologies have changed processes or people that concern their discipline’s ontology. So, there has been proliferation of terms like cyber politics, cyber sociology, cyber citizen and cyber criminals etc. They have talked about how cyberspace facilitates freedom of expression or frees one from the tyranny of heterosexual division of gender or allows people to participate politically and challenge the state. It even talks about how cyberspace gives birth to online multiple gender identities. These works have the normative assumption of what cyberspaceshould be doing or promoting. So, for instance when Tim Jordan (2003) talks about how cyberspace has empowered people participating in it by enabling them to create their own societies and multiple identities, he veers round to the view that human freedom should have this kind of freedom as well. In this regard, he finds human freedom to be constrained because of embodiment that physical world creates. Jordan feels that virtual world allows a person to come out of a fixed gender identity that is rooted in physical existence. He seems to carry the implicit idea that cyberspace ought to give privacy and freedom to an individual. His stance also compares cyber virtual space and the real physical space by attributing political and societal oppression of some persons to the latter as opposed to the former. As opposed to this, Hakken (2002) does not show an inclination to give an unambiguous opinion. He agrees that there are cyber actors who have agency but they are not out of their community they create. The so called computer revolution can still be doubted. Hakken is therefore a skeptic who will not see it in just one way.

Similarly, there is another skeptic opinion that says that the idea of cyberspace as a liberating space seems to suffer from technological determinism. Cyberspace is also not seen as all empowering because it excludes many and there is digital divide (Hurwitz 1999; Mossberger& Hamilton 2012; Warf & Grimes 1997; Froomkin 2003; Sylvester & Mc Glynn 2010; Loader 1998; Sassen 2002; Kennedy, et al 2003; Warf & Vincent 2007). Such opinion has some kind of predilection for equity. This indicates their assessment on how cyberspace governance should evolve further. Other skeptics see cyberspace doing limited benefits because of absence of same level of democratization everywhere (Best & Wade 2009), dangers of political universalism from cyberspace (Jones 1996) and trappings of state power (Polat 2005; Lessig 1998). So, the skeptics have diversity in terms of their normative assumptions. They are tempered by those ideas that see the better side of cyberspace more than its negative tendencies and implicitly mean to support the existing governance or absence of control of cyberspace. These too are prone to nurse vision of how cyberspace governance should or should not be. Included in this are the cyberlibertarians like John Perry Barlow who sees the virtues of cyberspace in the immense liberty it provides to everyone. That is why he has called it ‘liberating cyberspace’ (Barlow 1996). The distance from liberty to subversion is not very long, so cyberspace is also seen as a space where information flow is subversive (Starrs 1997). It is also said to have overthrown matter in twenty first century (Dyson, et al 1994), act as free source of information (Cahir 2004) and provide a space to the disadvantaged, dispossessed, religious communities and religious literature (Adler 2008; Alkalimat 2004; El-Nawawy&Khamis 2009; Azzi 1999; Lucas 1996). All these opinions can be said to stand on the assumption of a truly free cyberspace. But, is cyberspace really free? The study of cyberspace governance would reveal this. There are indeed several trappings of state that temper the freedom that has been talked about here. This brings one to the next strand in the literature on cyberspace which is state centric.

1.2.2 State Centric Approaches

It is quite an irony that there is large body of state centric literature on cyberspace although the latter inherently encourages movement away from state centric positions. State and cyberspace are not antithetical to each other. The proponents of cyberspace freedom seem to miss this fact. One just needs to remember that beginning of cyberspace lay in the military oriented experiments of United States in 1960s. Defense Advanced Research Project Agency’s (DARPA) efforts to develop rudimentary Internet are now a legend. Yet, it is surprising that eyebrows are still raised when states are seen to be tinkering with the functioning of cyberspace. Interestingly, a large part of the literature on cyberspace is state centric. Development of this strand in the literature has happened very gradually. These have covered basically three types of developments:

1.2.2.1 Militarisation Discourse: In simple terms, militarization discourse sees cyberspace as a site of conflict. This conflict involves state as well as non-state actors. So from conflict, the jump to warfare is a child’s play. Therefore, the militarization discourse has gradually proceeded towards warfare centric studies. Since military is seen as the most visible part of state machinery, cyber warfare and cyber militarization discourse has found a prominent place in state centric approaches. This militarization discourse has paid attention to those aspects of cyberspace governance that are related to military applications of it or help in tackling with it. So the result is a proliferation of terminologies that help in understanding cyberspace as an instrument and site of conflict. These terminologies form a bulk of cyberspace literature today. Scholars belonging to this strand have given terms like ‘cyber power’(Libicki 2009b; Starr 2009), ‘sub-rosa warfare’ which is more like a war in which there is no more a clear perpetrator of attack (Libicki 2009a). Libicki has called sub-rosa warfare as a warfare which not only takes certain types of attacks off the table but also lies below the level where either side has reason to escalate into at least explicit warfare. Libicki has provided another interesting term ‘cyberdeterrence’. Deterrence is a term which evokes pictures of nuclear conflict because of the well known association of deterrence and nuclear weapons in the nuclear warfare. Libicki indeed has come close to comparing the cyber deterrence with nuclear deterrence (Libicki 2009b).

Another kind of military centric approach explores even a more complicated arena which is the application of International Humanitarian Law to the cyber warfare. In this, Robin Geib (2010) and Jeffrey Kelsey (2008) deal with how cyber conflict affects the application of the International Humanitarian Law in the event of cyber war. Scott D. Applegate goes even a step further and corroborates with several instances his conclusion that cyber warfare indeed has the potential to become kinetic cyber war. He does this by citing incidents, in which cyber activity or a malware was detected, which if ignored could have caused severe injury or damage to the physical existence of individual or infrastructure. In fact, the case of Stuxnet virus is often cited while discussing such a scenario. Stuxnet was discovered few years ago by the Iranian authorities when they found out that a virus in the command system of computers that controlled nuclear installations, had made the reactor rods to spin out of control. What was the reaction then of several people? It was that such things could happen. So the possibility of kinetic cyber warfare discussed in the literature derives its nourishment from more recent events that undoubtedly corroborate them. Similarly, cyber terrorism has also received lot of attention in the military discourse in the literature. The advent of Al-Qaeda and its several splinter groups has become a great motivating factor in pushing forward cyber-terrorism as a concept. In this particular area, it has been found that terrorist groups are increasingly relying on cyberspace to inflict damage on their targets and therefore they need to be countered in this sphere with a sense of urgency. This will require a new understanding about the strategies used to spread terror in cyberspace and of the goals of attackers (Curran, et al 2008; Ariely 2008; Libicki 2007, Colarik 2006). The motives of cyber terrorism are determined by the same factors which play a role in terrorism elsewhere, that is, fear factor, spectacular factor and vulnerability factor (Janczewski&Colarik 2008). Therefore, Arquilla&Ronfeldt (1999) have called the dawn of cyberspace and its spread as a cause of major shift from realpolitik to noopolitik. They have derived this term from ‘noosphere’ coined by Pierre Teilhard de Chardin which means sphere of the mind. So, Arquilla&Ronfeldt have given a comprehensive picture of the change in global politics that involves shift in every sphere of the politics that is being played out in which states have to constantly employ ideas and interact with non-state actors even while remaining paramount actors in international politics. This brings one to the next strand in the state centric approaches.

1.2.2.2 Territory, Control and Sovereignty Centric Approaches

These approaches are quite diverse in terms of what they have to say about changes that cyberspace has brought to the institution of state and sovereignty. It has been found that the initial wave of reactions to the dawn of cyberspace technologies was oneof euphoria. It was natural on the part of many to feel exultant because new things became a reality. The celebration, however, gave way to the realization that it was not a creative force for all the institutions. No sooner had people congratulated themselves for having made a technological marvel than a realization dawned that it was actually chipping away parts of sovereignty. Certain changes had started taking place which were looking novel in terms of the way state could function. Naturally then, the question arose: What is happening to the sovereignty? Sovereignty is a contested concept as it can have several meanings. But in the common parlance, it means state control. Now, this control can be overarching, very minimal, moderate, and limited, all depending upon the nature of state, government and several non-state institutions. But when cyberspace expanded to include many more facets of human existence, it was found that it was playing by its own rules. States now discover that the commerce takes place in a very different way than it did in other physical existence. The novelty stumps them and it is felt that it is beyond laws of states. Cyber crimes have risen, compelling states to wonder about the nature of this zone. The sovereignty and the sense of borders seem to disappear. In the wake of this perception has come about an idea of 'deterritorialised sovereignty '(Shabazz 1999). Therefore, the first immediate response has been in terms of explanation of denudation of relevance of territory and borders, because cyberspace does not seem to operate on these principles. What matters are the advent of new forces that are causing these, namely, advent of netizens, online crimes and challenge to the earlier regime of commercial, intellectual and private property rights (Johnson & Post 1996; Katyal 2001; Russell 2008; Maloney 1997; Rosenzweig 1995). Hence, intellectual chutzpah would say that netizen is the new breed and citizenship has gone the dinosaur way. Terms like Blogosphere accentuate such perception. But the literature has skeptic reaction as well. There are arguments that not all is lost for the state and that the above kind of conclusion is partial and comes from a particular perspective. Firstly, according to Steinberg & Mc Dowell (2003), the argument that there is a threat to sovereignty emanates from a Realist perspective that has state and its sovereignty at the centre of its explanation. Thus, they fail to see other phenomena that may be happening gradually. Secondly, far from being antithetical to each other, state and cyberspace are increasingly developing symbiotic relation (Everard 2000) and non-state actors frequently collaborate with state actors to improve Internet Governance (Wilson 2005). Henry Peritt (1998: 424) also says that the 'conventional wisdom' that finds internet posing challenge to sovereignty can be questioned because Internet actually has the 'potential to strengthen national and global governance. He gives reasons that are informed by liberal theory of international relations. Firstly, Internet can contribute to international cooperation by strengthening international law. Secondly, it increases international economic interdependence, empowers NGOs and supports international security. Therefore, when seen from a perspective of international cooperation and interdependence, a state's powers and its sphere of functions seem to be changing if not shrinking.

There is another emerging strand in the cyberspace governance which, as the word emerging signifies, has remained in the government policy documents. Policy documents or white papers can be mundane and may appear to be lacking depth. But these are important parts of the literature because they carry much of how states plan to interact with cyberspace. Countries, particularly the developing ones, have come out with several plans to increase the digital literacy and reach to bridge the digital divide. Apparently, states want to utilize the digital technology to their benefit. In a state centric approach, these areas remain virtually untouched even though there is zeal to connect the length and breadth of the country. This indicates that it is only certain functions of state that have attracted the attention in the literature. Those are the military, security and surveillance related functions. The military and security issues have been already discussed. The reason for this tendency is that these functions of a state are regarded as the most visible forms of power and control. There are however several areas where the control by state is not either direct or takes place in a subtle and silent fashion, without attracting suspicion of even those who are wary of state apparatus. These are the areas of development and economy and morals. These are the places where state registers its presence in the cyberspace to govern. Yet these areas have not been explored enough in the available literature with the aim to extract out the state power and control apparatus. An instance can be cited here of how states can register their presence. Russian President was once asked a question about Internet. Not only did he call it a CIA project (which is not surprising, given the Russian leader's own security background), but also said: "On the Internet, fifty percent is porn material." That was not an off the cuff remark but was an indication of where he as a leader wished to take country's cyberspace governance. He was targeting the security and the moral issues that he thought were right. In an age that has freer flow of information in comparison with earlier years;governments are concerned about what their population reads and see. The reasons for concerns vary. In fact, cyberspace has the potential to provide controlling handle to the state. But this brings one back to the state. State, therefore remains a central point of analysis.

1.2.3 Theme of Cyberspace as a resource and global commons

A resource can be simply defined as something that can be exploited and utilized for producing something else, usually a finished product. A global commons is also a resource, but one without clear property rights. Oceans, atmosphere, the air we breathe, are all global commons. Due to lack of clarity on who controls these resources, the global commons often suffer from over exploitation leading to depletion of resources. In cyberspace governance discourse, there is a strand that analyses cyberspace governance from the perspective of its resource quality. Therefore, the focus shifts to the question: how is cyberspace used and what can be done to bring effective pricing of its use? This line of thought is being pushed by several in the corporate sector. In fact, many big internet players like Facebook, Amazon and Google were incubated in the period when Internet took wings and spread far and wide. These companies have flourished in a world that allows a free flow of information unhindered by any pricing structure that privileges anyone. Therefore, they see it as a resource that should remain free because that gives Internet its essence. But debates in cyberspace governance are interconnected and so what affects economics and business can be equally a concern for politics. Therefore, it is important to see points where several issues intersect. One such issue that has become a hot potato is the net neutrality. In simple terms, network neutrality means that the broadband companies will not discriminate between the information that is being moved[2]. Tim Wu (2003: 142) opines that it is often the argument of the open access that network neutrality fosters innovation while any kind of broadband discrimination by the companies on the basis of a pricing structure would kill the innovation in Internet. The reasons for this is that once it is allowed that a broadband company can provide better quality of speed to an information on the basis of payment, then many companies who have flourished on the basis of free flow of information may face discrimination and entrepreneurial tendencies may get curbed.

On the other side of this debate are the telecom giants like AT&T, Comcast and Verizon. These companies want to change the rules to allow them to discriminate between information on the basis of pricing model. The Internet giants of US with net worth that run into billions of dollars have given strong reactions to any attempt to change the rules to change network neutrality. The Internet Association

[2] Network neutrality ensures that one is able is able to go wherever one wants to go online and the network service provider will not either favour or discriminate against in terms of providing passage to the information being passed. An example can illustrate this. One can assume for a moment that a service provider is the fee collector at the gate for allowing the number of vehicles at a time. There are four parties with several vehicles desiring to pass through the gate. If fee collector allows a quicker passage to the party which pays more and asks others who pay less or no amount to wait for longer time, then the speed of parties' vehicles is being discriminated on the basis of the amount of fees. Somewhat similar is the case when network neutrality is violated and information flow is discriminated.

that is a body of 35 tech giants of US gave a statement that was a response to USA's Federal Communication Commission's attempts to seek opinion on network neutrality before bringing any change. The statement talked about preserving innovation potential and democracy. This is significant because with the talk of democracy, the discourse is no more confined to realm of economics and business. It is therefore not surprising to find that forum like Open Internet that wants Internet to remain a space of freedom of expression and innovation, has also popularized this debate. Its website has this written: "A free and open Internet is the single greatest technology of our time and control should not be at the mercy of corporations". It is not clear whether the word 'corporations' also includes the tech giants who also favour network neutrality. But the forum's views make it clear which corporations they are referring to. Among benefits of network neutrality, it counts competition among Internet Service providers (ISPs), prevention of unfair pricing, promotion of innovation, easy spread of ideas, increasing entrepreneurship and protection of freedom of speech. Therefore, the discourse is of interest to interdisciplinary research. This particular area however has not been explored much from that perspective.

The idea of 'free internet' and impact of commercialization on it' has however been dealt with. Saskia Sassen (1998: 545-547) opines that one cannot take the openness and democratic potential of Internet as given because it has become segmented and its spaces privatized over a period of time. According to her arguments, Internet has evolved in phases and in its earliest phase it was confined to a community of scientists and select government agencies. The second phase opened it up to people and it encouraged hackers to spread the open and democratic character of Internet. However, the space was soon discovered by the business sector and itsspaces. It is becoming increasingly segmented now. Sassen says that Internet has become "a new theatre for capital accumulation". Some have called it the "corporate colonization of cyberspace". According to this argument, cyberspace has the inherent tendency to promote free flow of information, free access to it and democratization of ideas. However, this tendency is being killed due to the financial muscle of the big media companies that dominate the information sphere in offline world. In this corporate dominated cyberspace, internet users are not users but consumers, who then are bombarded with links of news and advertisements (Sriskandarajah 2014). Therefore, the cyberspace as a resource for commerce and business is not seen uniformly. The big corporate are objects of criticism. Therefore, a cyberspace governance policy from such perspective is bound to be different from the one that sees that cyberspace isneither segmented nor is being appropriated for private uses.

1.3. Multiple Meanings of Cyberspace Governance

It has been found that there are many actors who have made sense of cyberspace and defined it. These meanings hold significance for the topic of this research because governance of cyberspace depends first and foremost on what it is that has to be governed. Due to lack of unanimity on certain areas of definition, the issue of cyberspace governance is an unsettled area. There is an opinion from open access activists who want no control. There are perspectives from states. States do not have one perspective. United States has one and so has Russia or China or India. The countries are still haggling over what the issue should comprise of. Then, there is an overarching presence of the corporate that have wished to bring regulations that benefit them. There is no unanimity among them either. There has been a predominant tendency to see meanings as mutually exclusive of each other which may not be so. For instance, increasing attempts by states to put in place a cyber security is seen as a movement of cyberspace governance in the direction of increasing state control. This state control is assumed to be opposed to interests of Internet companies who may have to face constraints on the ways they provide goods and services. But are interests really so mutually exclusive? The assumption of mutually exclusive interests and perspectives stands on the basis of mutually hostile role of state and the private sector. More recent events give enough fodder to question this assumption. It is now well known that the efforts by several states to improve cyber security are being fuelled to a great extent by the economic loss suffered due to theft of intellectual property, trade secrets and confidential policies. Companies have faced thefts that have proved to be costly. Recently, Sony Entertainment Pictures was targeted by hackers that resulted in exposure of several confidential details of the company and private e-mail conversations that were embarrassing. There was loss in terms of commerce apart from the negative publicity that the company’s cyber security system got. The popular theory behind the attacks has been that

Sony Entertainment Pictures was going to release a movie that had a comical treatment of a fictional assassination plot of North Korean leader Kim Jong-Un. The attacks therefore have been blamed on North Korea although the attackers have revealed their identity as Guardians of Peace only. The perpetrators threatened to inflict 9/11 style attacks. The association with North Korea brought into limelight the reactions of US government. Obama did react and termed the attacks as "cyber vandalism" and not cyber war as many were expecting him to and promised appropriate retaliation. Then, North Korea faced Internet outage. No one can be sure whether a small cyber conflict broke out between the two countries. But the focus undoubtedly shifted to what the two governments were doing about their respective losses. It is this kind of constant focus on the actions of state that have allowed states to acquire a very dominant position in cyber security discourse where they are seen as controlling and collaborating with the private sector. But as can be seen in this instance, the interests of two are not very different from each other. This is not the only instance. The governments of several countries and leaders have registered their presence in the social media. They own twitter handles and facebook accounts. Governments, ministries and leaders are now increasingly using the social media to make important announcements and for political pronouncements. As an example, there is India whose leaders' tweets are often seen in the cyberspace with many following them. India's incumbent Prime Minister is in fact an unusually social media savvy. He has welcomed several well known names from the Internet companies for the latter's developmental role. These instances indicate that states and Internet companies are not always on the opposite ends of the issue of cyberspace governance. There is much more ambiguity than the black and white argument that is often made out about interests of state and internet companies. However, this ambiguity has not been explored enough. As a result, one gets to see either states and sovereignty melting away or the gargantuan state machineries in countries appropriating the cyberspace. If it is not the state that is seen in the latter situation, then it is the corporate world which is described as such. After all, is the idea of corporate colonization of cyberspace not similar to state encroaching on cyberspace for expanding its domain? The only difference is that in place of state, it is the internet and media companies that are seen as playing the role of colonizer. The cyberspace governance is thus seen to be changing in an alarming fashion.

But it is important to see which set of practices and ideas lead to such a perception. In this regard, it is important to see the role of initial wave of liberal ideas of free cyberspace, unregulated space, egalitarian participation and access. This is because a very important pillar of cyberspace is the ideas and ethics that inform the fashion in which it has been operating ever since it has been commercialized. There are several thoughts in a whole spectrum of liberal thought that have termed cyberspace as inherently equalizing and free. In this spectrum, cyberlibertarians are on one end of the spectrum that see any sign of governmental or corporate control as damaging. Examples of the recent opposition to state laws and regulations for the online commerce and surveillance are there. Electronic Frontier Foundation, for instance, is a major platform for cyberlibertarians. It has taken out several white papers on a wide range of issues of cyberspace governance, from copyright laws for online content to the role of technology companies in perpetuating the oppressive practices in world’s repressive regimes. It issues white papers on these issues often outlining a libertarian perspective on the problems.[3] One of the typical examples of their activity is given in their website. They have listed several rights under their Bloggers Rights agenda. The rights are: Bloggers should have privileges and rights that journalists get as the bloggers can be journalists. They are entitled to free speech, political speech, have the right to stay anonymous and freedom from liability for hosting speech the same way other web hosts do. Therefore, the rights listed by EFF are aimed at strengthening the rights of very prominent members of cyberspace. Apart from this, the role of EFF is also noteworthy in the field of protection of privacy. Privacy is not taken seriously in several parts of the world and least by the ordinary users. It is this kind of complacency that EFF has sought to remove by spreading the importance of protecting the online privacy. One of its projects called HTTPs Everywhere is meant to encourage people to protect themselves against traffic analysis (which is a kind of surveillance in which the sites that a person visits, is tracked). Since it is the governments and their security agencies

[3] Electronic Frontier Foundation (EFF) calls itself a non profit organization that works for defending civil liberties in the digital world.

that are known for keeping tab on internet traffic, the program is meant to help users to avoid falling prey to such attempts. It is quite an irony that the partner of EFF in this is the Tor Project which began in the United States Naval Research Laboratory for protecting governmental communications. Tor is a technology that allows people to avoid traffic analysis (www.eff.org). Similar to the Electronic Frontier Foundation is the Technology Liberation Front. This second forum describes itself as the forum that seeks to undo the creeping role of governments all over the world. So, they are set against any kind of increase in governmental rules and regulations that takes away the freedom to choose and express oneself in cyberspace. This is premised on the negative effects of governmental interference on the freedom of expression and to choose. Their slogan which says "We fight for Tech Freedom", reflects their goal very clearly and loudly.

Apart from these fora, there are individual activists like Julian Assange and Edward Snowden whose cyberlibertarian streaks are very obvious. These are two most well known faces in this field who have borne the brunt of establishment and mainly states whose secrets they have helped in tumbling out. Out of the two, Assange has a hacker background. In a book written along with Suelette Drefus called Underground, Assange has told his story through a hacker character Mendax. According to Robert Manne, Assange became a part of 1980s hacking culture in Australia, the country of his birth. In October 1989, NASA computer system was attacked with a worm from Australia. The attack appeared to be a sabotage attempt at the Jupiter launch of the Galileo rocket for protesting against nuclear weapons race. Assange has given a hint that he was behind it. Later he also joined two other hackers-Trax and Prime Suspect and they named themselves the International Subversives. Their activities were anti-establishment and were within ethical boundaries as they made sure that they neither harmed the computers they targeted nor commercially benefitted out of their work. As part of their work, they heavily targeted US Defense establishment computer systems. Canadian telecom company Nortel was also attacked. He faced arrest when one of their partners revealed to the police the activities but was set free with a $5000 good behaviour bond and $2100 fine. His interests however took him further. He soon joined cyberpunks[4]who believed that in the tussle between state and individual, the individual rights will be the winner. The philosophy was attractive to the hacker Assange. The aim of cyberpunks was obviously to fight and preserve a free culture in which individual is not trampled upon by the state in cyberspace (Manne 2011).

The significance of Assange story does not lie in the sensationalism that accompanied when the Wikileaks, his organization that leaked to the world several classified documents, became famous. Its importance instead comes from the ethics and philosophy that compelled him to be what he is. Today, if there are any vociferous arguments against cyberspace governance, they come from quarters that are inhabited by many Assange. Any kind of governmental control is not just viewed with suspicion but is almost despised on the basis of ethics that see individual rights to freedom of expression and access to information as sacred. Edward Snowden who blew the whistle over the US National Security Agency's (NSA) extensive, deep and international surveillance program which involved cooperation of several Internet companies with the American intelligence agency, is also influenced by the cyber libertarian ethics. It is therefore not surprising that when he blew the whistle and went into self imposed exile, he made his motives behind his actions very clear. In a story covered by Glenn Greenwald, the Guardian journalist whom Snowden gave several classified documents, Snowden's mind was revealed. He has talked about the value of internet freedom that is being increasingly eroded by the state surveillance programs. He has talked about how NSA risked the privacy of citizens and others. According to the story, his laptop was found to have stickers that read: "I support Online Rights: Electronic Frontier Foundation" (Greenwald, MacAskill and Poitras 2013, The Guardian). Like Assange, he too trained himself in ethical hacking. He is said to have taken training from Koenig Solutions in New Delhi. Koenig Solutions is an authorized training partner for several computer and tech companies including Microsoft and Oracle (Phadnis 2013, TOI). More important than the backgrounds of Snowden and Assange are the things that they chose to reveal. They were

[4]Cyberpunks are skilled people with knowledge of mathematics and computer and use cryptography (encryption of messages) to achieve various goals like encryption of messages, decoding a secret, breaking into a site. In short, they can be hackers or code crackers and makers with or without political motive. These days, the word 'cyberpunk' is also used to express a culture in which technical skills are used to achieve political goals of civil liberties.

classified information. In case of revelations by Snowden, the things revealed were directly related to how US government was controlling the online lives of people in several parts of the world by subjecting them to widespread and indiscriminate surveillance. While Assange's actions reinforce the freedom that cyberspace inherently has by challenging the authority of governments to keep secrets, Snowden's revelations reflect clearly his idea of cyberspace governance that respects individual privacy. Assange in fact has been known to express his fears regarding dystopia that the governmental surveillance has bred in him. According to him, internet is a hybrid taking shape with governments and multinational corporations spreading their control all over. This tendency is likely to lead to global grid of surveillance. For the same reason, he is a dystopian about the future of Internet calling it a "threat to human civilization"(Morris 2013)

There are also hackivist groups and gatherings that are anti-surveillance, anti-establishment and have anathema towards anything that smacks of centralization. Their most popular targets are the defense and security establishments. The defense and security organizations are seen as symbols of centralized power and control. Anonymous and Lulszec, the two hacktivist gatherings who are known for hacking websites have targeted many government as well as corporation websites. These hacktivists are known for having political targets that are hampering transparency, centralizing or harming individual rights in some way. For instance, Anonymous conducted an Operation Payback in which they targeted anti-piracy groups who are opposing online violations of copyrights. The targets included Recording Industry Association of America, Motion Picture Association of America and Australian Federation against Copyright Theft. They inflicted Distributed Denial of Service (DDoS) attacks that disabled the targeted websites. The attacks were in response to the taking down of file sharing website The Pirate Bay. Before the attacks, the group wrote a message in which they expressed their disgust for the tendency of big corporations to control for their profits and resolved to stop the activities that discourage spread of ideas and attack the right to share knowledge (Winterford 2010). LulzSec, an offshoot of Anonymous, is also known to have targeted CIA website, Sony database, Tunisian and Egyptian websites during Arab Spring, Soca (UK's Serious Organised Crime Agency) website True to the ethics that they seek to promote, these hacktivist groups have no hierarchy and their way of operations is totally decentralized. They are however known to discuss strategies of attacks in Internet Relay Chat channels. They have no leader and anybody can join the groups (Coleman 2010). By expressing themselves anonymously, these hacktivists intend to give their most important message that they are for anti-authority, anti-leader and anti-celebrity culture. Also, anonymous expression promotes democracy seems to be the belief of these activists. If one talks of cyberspace governance, these hacktivists will be on one end of spectrum which is loathed to any kind of authority and control. What governments, security agencies internet companies, telecom companies and other film and media big corporations call cyberspace governance is actually viewed with lot of suspicion by these. Governance will not be a word in their dictionary. The middle of the ground debates on cyberspace governance cannot be conducted with these types for the conclusion is unlikely to arrive. Hacktivists have a set of ethics as their base which is quite unlike other participants like governments and corporations who have entirely different set of concerns.

Despite this inability to find a concurrence, the libertarian practices even of very extreme types are important part of cyberspace governance because some of these elements are being pushed into a periphery status. Government and corporation driven discourse has created new meaning of internet freedom and egalitarian cyberspace. This has proceeded at a very gradual pace through practices and pronouncements. The discourse has put to the fringes the earlier cyberspace ethics that these groups like Anonymous have kept alive. What dominates today is cyber security, cyber policing, protecting online copyrights, surveillance, e-governance, and biometrics. Any DDoS is viewed as act of cyber war or at least cyber 'vandalism' as Barack Obama called when hackers attacked Sony Pictures Entertainment. 'Vandalism' is not a term which is used for an accepted member of society. It denotes loot, mindlessness, aimlessness and reckless behaviour. In other words, it denotes a class of fringe elements whose behaviour is unacceptable and punishable and deserves no serious consideration. It is not surprising therefore that whenever any attack of DDoS attack takes place or any site is defaced in which a leader or organization is made fun of, the attacks are added to the list of cyber crimes. Therefore, it is quite an irony that cyber libertarian streaks that initially influenced the cyberspace related thoughts and was the reason for defining the euphoria in the initial wave has been supplanted by new meaning. The ‘new mainstream’ has co-opted only those elements of cyber libertarianism that are not harmful to the growth of new mainstream. Those co-opted meanings are often fielded in arguments by several actors to promote practices that are gaining prominence in business and governance.

1.4. States and Corporations, the New Mainstream: Where is it headed for?

It is the new mainstream that is everywhere. It does not need to argue because it has become a mass of mainstream meanings. The actors who have been pivotal in creating and reinforcing these meanings have been the state actors and numerous corporations in the internet field, security industry, commerce , software majors and tech companies. Their concerted efforts have led to the point where they have ‘some’ level of consensus. As the word ‘some’ indicates, it is not a full, across the spectrum consensus. For instance, governments around the world may be more inclined to keep their population under surveillance than Google or Facebook or Twitter. But these corporations may like to cooperate with states over use of social networking by terrorist organizations or fraudulent money transfers or any kind of pornography. Similarly, hacking may be seen as a problem by the intellectual property creators as well as states. Therefore, with some differences and some consensus, the actors are driving the discourse.

The important point which is also main theme of this study is the direction in which this discourse is headed. So, is one going to see the whole thing revert to complete control of cyberspace by states that splinters the whole thing? Or, is the world going to see the corporations everywhere with cyber citizen reduced to cyber consumer? These are indeed very extreme scenario. Only time can prove or disprove the two or either of the two. However, it does not prevent this study to argue that firstly discourse has a wonderful quality of evolving itself. It can be headed in a direction but it cannot have an end because then it cannot evolve in the first place. Also in such a case, ideas will fall apart and new ideas will come out of the blue. That sounds implausible for a discourse. With this assumption (which has its limitation because it sidelines other definitions), this study argues that cyberspace discourse by mainstreaming governance is actually headed for a consensus over control by states.

1.5. Consensus and Differences

On governance of cyberspace, there is a consensus on one need and differences over how to meet that need. It is exactly like a few people desiring to go to one place but disagreeing on how to reach it. It can be argued that ‘consensus on the need’ is all that matters and the differences afterwards are not that much of an issue. The real problem however lies in latter differences as well as in the way initial consensus has been arrived at. This is because initial consensus on the problem precludes several other questions that can be allowed to grow or in other words, differences are permitted only on ‘agreed issue’. The rest is the fringe that does not form the main point. Therefore, a great part is silenced.

Therefore, the differences today seem to be having common theme. For instance, the funny aspect of the revelations by Edward Snowden was how countries reacted to all the exposed activities. United States stood as someone who had been stealing things all along but had now been caught. While US leaders were outraged by the actions of their compatriot whistleblower, the countries seemed to be less outraged by immorality of American actions and looked envious of what US had achieved. What pained them was the fact that US had dared to step in their domain. While Brazil leader Dilma Rouseff gave a stinging rebuke to US in her UN speech calling it “a breach of international law and an affront to Brazil’s sovereignty, she also argued that there could be no real freedom without the right to privacy and also said that there could not be a basis for proper relations among nations without respect for a nation’s sovereignty (Lynch 2013, The Washington Post). The revelations had brought out the embarrassing fact that United States had been conducting surveillance on Brazilian oil major Petrobas which is a state owned company. Dilma Rouseff reacted not only by giving a piece of her mind to United States but acted swiftly to introduce a law which is popularly called Internet Law. It is actually named Marco Civil da Internet. After signing it into law, she once again emphasized that Internet that was desired was possible in an environment of respect for human rights primarily privacy and freedom of expression (Toor 2014). Brazilian law has been described as Brazil’s internet bill of rights because of many principles that it has enshrined one among them being net neutrality. It also ensures that Brazil’s internet users’ online privacy as it bars searching the data. Freedom of expression is guaranteed in a provision that requires a court order to force removal of contentious content. But it also expands the reach of the law to any internet service in the world with Brazilian users. For example, a firm in another country whose services can be used by Brazil’s citizens can be penalized if it violates the Marcos Law. According to internet scholar Sergio Amadeu, this law may make the Brazilian users data more vulnerable because the country does not have a comprehensive data protection law. This mayactually make it easier for the government to sift through the citizens’ data (The Economist 2014).This sounds strange given Dilma Rouseff’s pronouncements on the civil liberties, especially right to privacy and free expression. But it will be easier to understand Brazilian stand if one takes into account the main reason for the country’s outrage which was the US encroachment on sovereign areas of other countries. Brazilian oil major on which US was keeping tab is known for playing a very important role in the country’s oil diplomacy. Its state ownership enables anyone keeping surveillance on it an easy access to the government’s sensitive information that can be exploited for gaining an edge in any negotiation. No wonder Brazil showed alacrity in instituting a law.

Other countries also showed concerns regarding the question of sovereignty. Indian reaction however showed no alarm. When it was revealed that India figured along with other major NSA targets Iran, Pakistan, Jordan and Egypt and that around 13 million pieces of information were scooped in one month only, Indian reaction was that it was not actually snooping and that countries spied on each other all the time (Aaron 2013). The WSJ found the logic behind India’s uniquely mild response in the country’s own aspirations for the surveillance capabilities. The report titled ‘India’s snooping and Snowden’ reveals why India should be mild. It talks about the Central Monitoring System that enables interception of all phone and internet communications bypassing the service providers (Bajoria 2014, India’s Snooping and Snowden). Reactions from China were along the lines of cyber security. Industries in China are grappling with cyber breaches and the revelations that US NSA hacked into Chinese internet traffic hubs and cellphone companies only added to the sense of urgency. Demands for a national strategy to protect information sphere have arisen in the wake of revelations and some in the industry are jokingly saying that they all should be thankful to Snowden for showing the vulnerabilities (William Wan

2013, The Washington Post). Later reactions that can be said to have come after an afterthought included expression of concern from the official side. Chinese Foreign Ministry spokesperson told that China was extremely concerned about NSA snooping and demanded an explanation for US agency's actions (RT 2014). In fact, when Snowden was in Hong Kong which is a special administrative region of China, China's Foreign Ministry suggested a cyber security working group to increase dialogue, coordination and cooperation (Schwartz 2013). Therefore, the Chinese policy makers seemed to have found an opportunity to formalize what had been taking place all these years that is a new theatre of security and diplomacy. It was more like the Indian reaction, which is more interested in putting in place its own cyber security strategy. China was therefore concerned but not outraged like Brazil or Europe. Europeans poured strong reactions expressing their fury over the revelations that some European countries were placed alongside countries like Iran and Saudi Arabia in terms of frequency of snooping conducted. The fact that European countries like Germany, France, Italy and Greece were targets of NSA despite their status of US allies added to the European allies' shock. Words like 'deeply worried', 'shocking', and 'unacceptable' were used to express the reactions (Levs &Shoichet 2013). Unlike many who ranted about the sovereignty, European countries felt more the sting of the backstabbing. Did it mean that they had no objections on ethical grounds of rights and privacy? Afterthought may bring a more sober reaction but it is often the immediate reaction that reveals the real problem. Therefore, Brazil, China and India reacted with their interests in their mind, disagreeing only to an extent which met their political interests. Europe's shock was more due the notions of allies that was present in their mind.

The interesting thing about the reactions is that they were actually not about the ethical soundness of the NSA actions but more about 'why me' reaction. Such reactions leave enough scope to do what the US agency did. In fact, USA has not been alone in all these surveillance programs. UK placed data interceptors on the fibre optic cables that carry data in and out of UK. This was done as part of Project Tempora of GCHQ, the country's intelligence agency that collects intelligence information, which is a British counterpart of NSA (Shubber 2013). The activities of Five Eyes that collaborate in collecting and sharing intelligence have also revealed that countries like Australia and New Zealand too have facilities to intercept the internet traffic. According to Snowden, they have been found to have few steps further than NSA on several occasions (Dorling 2013). It would therefore be farfetched to conclude that Snowden revelations enabled countries to develop a consensus on privacy rights. Instead, the cacophony of countries over US actions hides the other consensus that has gradually developed and that is that cyberspace is not something that can be left untouched. That however does not mean that countries have arrived at a definition of ‘control’. It has been left vague by those who are inclined to control which in this case are states.

The word control is therefore a contentious area in the literature. The furore over NSA programs does help in understanding certain practices that can define the word but they are not the only things that go into control. Conditioned by system that inhabits a country, a state can employ any kind of control over cyberspace. That may or may not include surveillance activities. A state whose writ runs in all spheres of citizens lives including the private sphere may feel that it is total grip over the use of internet that can be called control. But a less stringent requirement is likely to make up the definition of the word in a country like USA because the people may simply find surveillance incomprehensible and reprehensible. Most importantly, there is a need to see that all are not comfortable with the way cyberspace carries most of the American baggage and influences. This means that Cyberspace governance is seen suspiciously by some countries because it does not represent the interests of the people and governments that do not belong to the developed world.

1.6. Internet Governance: Questioning the Status Quo?

An international conference was held in Budapest in 2012 in which it was noted by some delegates that many internet users had not been represented and that it was hoped more Asians and Africans would attend. Chinese delegates seized upon this observation to argue that cyberspace governance now needed to listen to new users from China and other Asian countries. They were, therefore, questioning the status quo in the way cyberspace has been controlled by US led west. Their remark that China had more internet users than any other country was symptomatic of a country that wished to chart a new course. The fact that invitees to the conference not only had several intergovernmental organizations but also NATO, OSCE, Google, Microsoft, AT&T, many ICT vendors and civil liberties and human rights organizations obviously gave it a liberal tone. Chinese and Russian emphasis on the need to defend sovereign control over cyberspace and preventing its uses for meddling in affairs of other countries undoubtedly questioned the liberal order of cyberspace. This kind of questioning may look to be veering towards the kind of diversity that cyberspace is said to be promoting by giving voice to new powerful players. But this conclusion has holes if it is made in present times. Questioning of US dominance does not imply anywhere more protection of rights and freedom. On the contrary, one may miss the fact that it will lead to dethroning of one and crowning of another. Meanwhile, the idea of control flourishes and gets entrenched. How else can one account for the increased sovereignty over cyberspace if not by splintering the latter? Therefore, this kind of questioningthe status quo does not overturn the logic of state control which is going on now. But such pronouncements and the practices further put into history books the 'ungovernable' cyberspace. This means that cyberspace has been already conquered. But the conqueror is not a state or group of states but the collectivity of ideas and practices that have gradually co-opted the realm of commerce, military, security, taxes, rules and regulations, laws etc. China's, and similar stances of other states only seek to extract benefits out of this co-opted entity by further strengthening the conquest.

However, states are not the only ones who are doing to govern the cyberspace. The consensus on control by states is not the only thing in discourse. Cyberspace too in turn has been co-opted by other human institutions as well and the most visible of all these is commerce and business. They are probably the other driving factors in the governance discourse but their role in the cyberspace is much more ambiguous than that of states. States can be very conveniently accused of controlling the things in cyberspace. Such battering cannot be done to commerce and corporations. It is because they have suffused into lives of people so deeply that psychologists are now claiming that their research on human behaviour indicates that people have developed addiction to the smart phones. With such users and addicts, internet companies only have wide reach to influence people. E-commerce businesses like Amazon, Alibaba, Flipkart have started not just businesses but have also given a message that the world is open to the netizens and they need not be bothered about the limited choices. Cyberspace is thus seen as a very positive force that connects a good from a country to a consumer in another part. Similarly, Google has become a symbol of open accessibility. It is no more just a search engine. Its reach and ubiquity in the cyber world has been no less powerful than any country'smight. The irony is that even the states that are usually seen inclined to kill off the cyberspace goose to take away all the golden eggs are actually enthusiastically encouraging the internet companies. US State Department only recently hosted Google+ hangout in 2014 (Google Blog 2013). India's incumbent Prime Minister is a twitter enthusiast what with his all ministries being ordered to go the social media way (India Today 2014). These instances are just few and reflect the deep reach of the internet giants. With such a system, the feeling of freedom is bound to permeate people and usually this has been mistaken as signs of non-hierarchical system in which a user at one end is as powerful as the company which is helping him access information in the laptop. The role of Twitter and Facebook in fuelling protests and creating a groundswell of opinion against autocrats in Tunisia, Egypt and Syria has already been noticed by many commentators, media platforms and governments. According to David Wolman writing in *Wired*, terms like Twitter revolution and Facebook revolution would be ridiculous because it is people who bring revolution. However, he argues that the two social media platforms played a significant role in accelerating the downfall of autocrats in some Arab countries. People had been protesting online and planning strategies by communicating through these media. The autocratic regimes did crack down on these but the nature of the clamp down was inept as the governments simply stopped internet and telecom services out of desperation. This only brought the people on the streets, accelerating the protests (Wolman 2013). Rebecca J. Rosen (2011) argues in the Atlantic that the question of role of Facebook and Twitter in fuelling and enabling protests has been largely theoretical with less of actual facts being brought to light. She feels that the matter has been 'fuzzy' because details have not been used to back up a theoretical argument. Reviewing John Pollock's analysis of the issue, she explains the role of an organization 'Takriz' started by two activists Foetus and Waterman (pseudonyms used by activists) which was actually a cyber think tank in its initial stages. The organization used hacking and social media platforms to communicate with each other primarily because of the anonymity that social media provide (Rosen 2011). Therefore, cyberspace has expanded its reach even in the corners of the globe where autocracy does not allow any dissidence thanks to some companies that have made a business out of human need to connect. It is however more the human ingenuity that has made the social media an instrument of protests in this case. What would any platform be without its participation? Despite this fact, it is the social media companies that have attracted the most attention. They have become important symbols of freedom and sharing. It is this kind of goodwill that they have acquired over a period of time. This would not be possible without all that freedom that they apparently provide without any blockading. This thing has to be taken into account in understanding cyberspace governance because any kind of regulation in the form of cyber crimes and commerce laws is likely to touch upon or encroach on what is currently being offered and being taken for granted. For instance, the Snowden revelations tell that USA's Foreign Intelligence Surveillance Act enabled the US federal government to demand direct access to the e-mail, video and online chat. This has obviously fuelled all the concerns about the safety of the private data in the hands of companies that handle social media and internet services. Apart from these concerns, the tech industry became wary after revelations. According to Information Technology and Innovation Foundation, a US based think tank, loss of around $35 billion was predicted by 2016 for the US cloud computing[5] business. Forrester analyst James Staten also estimated that Internet service providers would take a net loss of around $180 billion by 2016 (Gustin 2013). Therefore, it does not make a business sense to support any kind of governmental actions that would compromise privacy. Poor standards of privacy can mean less business from corporate that have many confidential things that are not meant for public consumption.

The Tech and Internet giants have raised a banner of revolt against the complacency in the system that allows governments to peep anywhere. Outrage

[5] The principle of cloud computing is the sharing of resources through internet rather than having local servers and personal devices for handling various operations. In cloud computing, the cloud is used to describe metaphorically the internet. Therefore services like storage and servers and others are delivered through Internet.

has been expressed by none other than Facebook and Google executives. In a low profile discussion held by Senator Ron Wyden who sits in Senate Select Committee, the tech giants' executives expressed opposition to the existing practices which have been led by USA. Google Chairman Eric Schmidt told that the happenings had broken the trust between American companies and other countries and that the same was making it difficult to do business. They also expressed that increased distrust may prompt many countries to go for data localisation[6] which means that they would be asked to store data in their own countries. Fears were expressed regarding how such a step would prevent most of them from operating on a global scale and would change the fundamental architecture of the Internet. Ramsey Homsany who was general counsel for Dropbox almost summed up the concerns in a crisp observation: "We have built this incredible engine in this region of the country and mistrust is the one thing that starts to rot it from inside out." (Chang 2014). However, the tech giants also sent united stand in 2013 through a letter addressed to US leaders and signed by big names in technology and internet, like Microsoft, Apple, Google, AOL, LinkedIn, Twitter and Yahoo. This called for reforms in government's surveillance programs and practices in the globe and said that balance was tipped too much in favour of states presently and away from individual rights (Timberg 2013).The perception of these companies is not accurate from the perspective of countries that do not have Internet and Tech giants in their territory nor is it shared by many anonymous hacktivists. The latter's anathema to corporate control of Internet has already been pointed out. This is because although it talks about Internet architecture, preserving it and individual rights, it takes into account only things and values 'that would make business sense'.

The fear expressed by these giants has been conveyed to and absorbed by US President. That is why President's first paragraph in the statement backing net neutrality is devoted to American economy and democratization. It goes like this: "An open Internet is essential to the American economy, and increasingly to our very way of life. By lowering the cost of launching a new idea, igniting new political movements, and bringing communities closer together, it has been one of

[6] Data localization means storing data in a data centre that is physically situated in the country in which the data originated. This has been favoured to prevent hackers from gaining access to the information that is data originating in the country that is going for local data centres.

the most significant democratizing influences the world has ever known."(www.whitehouse.gov/net-neutrality). At the time Obama endorsed the net neutrality, the President's opinion and statement was widely reported and continues to be reported. Whenever the issue comes up, Obama is quoted or talked about. Recently, when Indian telecom service provider Airtel sought to introduce the price pack in which VoIP services (Skype, Viber etc.) would be charged much more than other services, there was an uproar. According to popular arguments, this pack was a violation of net neutrality. The company had to withdraw the pack. But what was of interest was the way Obama's statement of net neutrality was reported in India. India seemed to have very small clue about the issue at that time. For it, US became the precedent. Therefore, USA has sought to wrest back the first mover advantage that it always had in Internet industry governance and which it was losing due to outrage over Snowden revelations. By giving an emphasis on the values of the country, it has shown it is still there to look after the Internet architecture and governance and of course to lead. But this is not the decade of 1990s. Alternatives are cropping up with entirely different sets of values as their bases.

1.7. Russia in Cyber Literature

Since, the point has arrived at which one can look at the alternatives discussed earlier, it is important to bring Russia into the picture. Russia does not have an edge the way United States had and still has in matters of Internet. It is still cognizant of the threats and opportunities that it is providing. The fact that Russian President calls it a CIA project goes on to project Russia's feeling that it considers the whole thing or network as alien. That kind of attitude is not unfounded because the speed the US picked up by developing the network in its labs and spreading it to universities was missed by Russia. World Wide Web developed in West, Facebook was born in the same country and so were the countless number of Internet and tech giants. US got the first mover advantage in terms of shaping its architecture, its culture and to a large extent even the kind of controls that countries are employing. The fact that US was found to be conducting a global surveillance shows that it knows the space inside out, an enviable position which countries like Russia covet.

However, it is wrong to reach a conclusion on the basis of this apparent drawback that Russia has a nil account in the information technology. It has some of the famous names in its territory. Kaspersky is a household name primarily because of the software security that it provides. It is famous for its cyber security research carried out in its own labs. It is located in Moscow and operates in 200 countries. Among its global partners are names like Microsoft, Cisco, IBM, Alcatel Lucent, Lenovo, Facebook, Qualcomm and BAE Systems. According to its own website, it provides various intelligence services to the government and private organizations like corporations. These services consist of forensic analysis of malwares and their analysis, providing early warning by giving raw data feedback to governments and telecom companies, tracking botnet activities and providing intelligence reports about regional variations of cyber threats on subscription basis (www.kaspersky.co.in/about). It has tracked several malwares, detected many and found out through forensic studies their origins.Its reports in the form of security bulletins form an important part of the cyber security literature. In the year 2013 which saw revelations about NSA surveillance, it brought security bulletin with the starting theme of surveillance, cyber espionage, cyber extortion and privacy (Kaspersky Security Bulletin 2013). Russia's MTS is also now a well known brand in telecom with the company providing mobile services in Russia and CIS countries. It has now extended its reach to India also. In 2008, Sistema (who owns MTS) partnered with Shyam teleservices and is providing mobile services under the same brand (www.mtsgsm.com/about/). The importance of this company to Russia can be gauged from the couple of occasions on which problems relating to Sistema's MTS were taken up by none other than Russia's foreign policy czars. With Russian government having stake of 17.14 percent in Sistema, the issue could not be taken lightly. In 2012, when Indian Supreme Court cancelled several mobile licenses over 2G spectrum corruption charges, Sistema ShyamTeleServices's telecom license was also cancelled. Sistema threatened to seek billions of dollars from the Indian government in damages. The issue became irritant what with Russia's Deputy Foreign Minister Dmitri Rogozin compelled to tell India 'not to reconsider the rules of the game once the game has begun'(Phadnis 2012). Russian Foreign Ministry also took up the cause of the company when Uzbekistan cancelled the license of a subsidiary of MTS and took into custody one of its senior executives in 2012. Russian Foreign Ministry expressed its concern and called the actions of Uzbekistan ‘severe sanction’ (Gazette of Central Asia 2012). Such interventions are of significance as Russia tries to increase foothold in the information technology sector. The spread of smart phones which are the point of access to internet and participation in cyberspace makes roles of telecom companies important as they are the ones who provide broadband services. Improved share in global telecom market is likely to give it larger heft in cyberspace governance discourse. Thus, Russia’s sensitivity to any infractions related to the same has a cyberspace governance angle.

Apart from some of these contemporary developments, Russia has an important aspect which would prove crucial in playing catch up game with US and west who lead in cyberspace governance discourse. It is the country’s deep understanding about the sphere of information that aides in understanding cyber sphere that is apparently in no one’s direct sovereign control. Russia has attracted attention in the cyber literature mostly in spheres of cyber security. Years of practical experience gained through several events of warfare has provided it a past to utilize to understand its position today. According to Edward Lucas (2014), Russia has been waging information warfare through its television outlet RT. The more you doubt, the less you trust, is the premise on which Russia has been operating in his opinion. This kind of assessment should not be surprising at all as the country already has a well defined information warfare doctrine. Peter Pomerantsev has explained that Russia’s information strategy has been underestimated. He argues how General Philip Breedlove’s (NATO’s top commander) statement that Russia was waging the most amazing information warfare blitzkrieg they had ever seen in the history of information warfare, was an underestimation. According to Pomerantsev, Russia engages not just in disinformation, leaks, forgeries, lies and cyber sabotage but also reinvents reality and mass hallucination. The observation is backed up with analysis of Russia’s information tsunami to counter west on Ukraine issue (Pomerantsev 2014).

Thus it is the information warfare in the context of which Russia is discussed. Of course, much of it has to do with what the country has been doing. Its cyber attacks are also not new. Soon after it had started emerging from shocks of Soviet disintegration, it allegedly targeted US Defense computers by intruding into them. The origin was traced to an ISP in Russia and has been recorded in history of cyber warfare as Operation Moonlight Maze(Joyner andLotrionte2001:840,841; Abreu2001; Drogin1999). Russian hand was also found in the cyber attacks on the Estonia cyber systems in 2009 over upsurge of anti-Russia sentiments there. The banking system got paralyzed for hours (Davis 2009). Then there was also cyber campaign against Georgia in 2008.According to Hollis (2011), Russia launched a consistent cyber campaign against Georgia at the peak of Russia-Georgia war in 2008 that involved DDoS attacks and defacement of websites. This campaign involved use of trained hackers and patriotic groups. In addition to all this, Russia was found to disrupt NASDAQ with a malware that apparently was meant to extract information and conduct surveillance but was found to be meant for disrupting the stock exchange. These well known cases with Russian imprint only bolster Russia's place in cyber warfare and security literature.

Cyber Warfare and Security however are not synonymous with the cyberspace governance. Of course, it can be argued that the state centric perspectives that have been discussed earlier gives a comfortable place to Russia. Understood in that sense, Russia's cyberspace governance is reduced to security and warfare affairs. Governance on the contrary and more so in case of cyberspace entails role of several other actors and even ideas. The latter is much more subtle and gradual. It does not have an explosive impact the way Russian cyber attacks bring to their targets. Russia therefore needs to be exposed to other aspects in the literature that can be as crucial as any information doctrine.

1.8. Significance of Russia as a Case in Cyberspace Governance

It has been found that several strands of thought and analysis centers have grown in the literature on cyberspace. The freedom and novelty induced euphoria has given way to talk of surveillance and protection of privacy. As mentioned earlier, cyberspace has been co-opted into the human institutions. There are now cyber crimes, cyber laws, cyber militarization, cyber security and even cyber espionage and extortion to talk about. There are even concepts of cyber-soldier, cyber weapons and cyber arms race[7] with vague meanings. One of the few things that

[7] At a conference held in Georgetown University, Director of Intelligence at US Cyber Command, Rear Admiral Samuel Cox said: "What we're looking at is a global cyber arms race. It's not proceeding at a leisurely or even linear fashion but in fact is accelerating. I wouldn't claim that it's following Moore's law, but the curve looks kind of similar." Moore's Law says that along with the exponential increase in

does not have cyber counterpart is the cyber or virtual state. States have found new terminologies to understand a new space they are compelled to operate in from time to time. But they have not allowed any parallel in the cyberspace to emerge however many may feel that cyberspace itself is like a state. The latter is not the case in the fast developing concept of cyberspace governance. Cyberspace governance is what states are employing. The discourse on the governance themes is at a point when broadly two models of governance are contending with each other. One is a model that has sovereignty as its core point. This implies a model in which all the cyber laws related to society, polity and businesses will be made with the aim to assert sovereign control. In this, issues of privacy and rights will be subject to the interests of the country and will not be upheld for the sake of protecting values. The second model is the one which believes in collective effort of all participants and actors to uphold the freedom of innovation, expression and to allow businesses to flourish. There is no clear cut border between the two as countries have been found to endorse features of both. But it is important to see that scales are tilted in favour of the former in the wake of many recent events. Some actors are however keen to see to change.

Is Russia one of those actors who are inclined to splinter the Internet? The answer to this has implication for the way governance of cyberspace is pushed. It is also important to see that the country is very much part of the wave of change that has swept the cyberspace. It is alone neither in pronouncements of greater control over the cyberspace nor in utilizing it to promote its own interests. In the second model of the governance, certain areas are sacred and cannot be touched. They are regarded as fundamental for the cyberspace. For Russia, it is not a hands off policy. Anything can be twisted to shape for the country. The moot question is whether Russian position changes the discourse by throwing off the pedestal the idea that cyberspace is ungovernable under the sovereign laws either due to practical implications of such arrangement or due to its unethical nature. In other words, it is important to see whether Russian position changes the discourse.

Russian position has significance for the direction that cyberspace governance takes at the global level by virtue of its potential in providing an alternative to

information technology capabilities, the potential threats posed by those technologies also increases at a sharp pace.

countries that are not acclimatized to the political system in US and western democracies. After NSA revelations, countries have got good excuse to crack down on the anarchic features of the cyberspace. The meaning of anarchic elements may differ from country to country, leading to various levels of control. Despite this, United States still leads in areas of corporate participation, innovation and cyber security industry. By setting up a cyber command, it has taken the cyberspace discourse to a new level by emphasizing its security aspect. Its tech and internet giants lead in net neutrality debate influencing ideas in far off countries like India where the debate over the issue is not understood much. On the other hand, the ideas led by US do not have an alternative leading to a situation where the idea of ungovernable cyberspace still prevails. Therefore, it is understood what all can be talked about. China has been seen as country that is engaging in cyber aggression with US having raised the issue of Chinese hand in increasing cyber attacks on US corporations and governmental machineries. Russia too has been bracketed in a similar fashion. The NASDAQ cyber attack which many called 'placing of digital bomb' did nudge US to wake up to Russian potential. The country was branded a potential source of cyber threats, coming as it did after cyber attacks on Estonia, Georgia and Ukraine. The country has also been vocal against US domination in cyberspace. If Russian model of cyberspace manages to destabilize the predominant ideas and practices by giving a valid alternative, a new norm emerges with new set of practices that then become perfectly normal and beyond the question. Therefore, Russian practices in cyberspace governance have significance for the norms that are developing.

Secondly, when it comes to norms, there are often the champions of norms. As an example, there are non-proliferation champions and so are the human rights champions. Cyberspace as a free global commons has its champion in many corporate and western democracies. Control of cyberspace by states has gained pace but without anyone championing it. As it has been mentioned, certain things have not been normalized in the discourse. Even China, which challenges the status quo, has argued for the international control of Internet. It is important to see whether Russia leads an alternative.

1.9. Framework for the Analysis

The main framework within which the study analyses various problems can be called Invention-Innovation-Practices-Spread- Entrenchment (IIPSE). Whenever there is invention of something, it comes into use only when it is improvised to meet certain needs. This minor or major improvisation is innovation. Innovation then leads to creation of several practices which spread and become common or entrench themselves in the society. From here, new innovations or inventions may take birth starting the same cycle again. In case of internet too, this process can be seen. Internet was born as a technology. It is however the human-machine interfaces that has led to many innovations. These innovations have made Internet what it looks like today. However, every interface, every need has led to an innovation in the form of new use, applications that in turn have given birth to new practices. These practices can be seen in political, social, and personal sphere. The spread of these practices have become fast and now some of them are well entrenched. Cyberspace governance needs to be analysed in the context of this framework because many of the issues relevant to it would not exist if there is no innovation. It is invention of social media, its innovative use, its spread and entrenchment that has resulted in issues of civil liberties in online space, idea of freedom in Internet, idea of threat to information space of a country and even free sharing of resources like copyrighted books. Without all these, countries would have been grappling with old issues by now. That many of the countries have shifted their sight to dealing with cyberspace itself is a sign of IIPSE framework at work. Cyberspace regulation which will be referred to in many places in this work is a result of certain innovations giving rise to practices. Surveillance by governments is also an example of state led cyberspace regulatory practice that has its roots in invention of online surveillance technology.

1.10. Methodology

1.10.1 Analytical Study

This study is analytical in nature, analyzing the data to subject two hypotheses to scrutiny. The two hypotheses are as follows:

1. Russian position on regulating cyberspace transforms the focus of cyberspace governance from ungovernability of cyberspace to cyber control by states.
2. Russia's notion of regulation is informed by presence of online political activism and cyber crimes in Russia.

1.10.2 Independent and Dependent variable

a) Position on regulation of cyberspace: This is the independent variable in the first hypothesis. In this study, the regulation is understood in terms of laws, rules, restrictions made by the government for uses of cyberspace and the uses of cyberspace by state like the use of cyberspace for surveillance and for warfare. The latter is a regulatory practice as state's very presence as a user brings an overbearing control over information sphere of the country.
b) Focus of cyberspace governance: This is the dependent variable of the first hypothesis. The change that the independent variable is hypothesized to cause in the dependent variable is in terms of shift from ungovernability to control.
c) Notion of cyberspace: This is the dependent variable of the second hypothesis.
d) Online Political Activism and Cyber crimes: They are independent variables of the second hypothesis. The online political activism is understood as participation of Russians in Internet through social media. The cyber crimes include crimes committed in/ through cyberspace.

1.10.3 Data, Resources and Analysis Technique

The foremost data for this study is one's observation of what actors are doing. Data of this nature are found in several places: newspapers, reports, and secondary sources like journals, books, and pronouncements of people relevant to the topic, pictorial representations, letters, correspondences, events, statute books and simply the day to day activities of the actors involved in the process. There are many actors in cyberspace discourse, from states and large institutions of NGOs, intergovernmental organizations and fora to small unknown or anonymous groups. Everyone is contributing to it. The data, therefore, are of texual and non-textual nature.

1.10.4 Analysis Technique for textual data like speech, actions and reports

The important part of this analysis is the context of speech, actions and reports. The context in this kind of study will look at the audience the person/actor was addressing, the events before the speech or non-speech act. For instance, a country has been in conflict with a neighbour. The two exchange some cyber intrusions for some days. Around the same time, a conference is held to look into new models of governance of cyberspace and the two countries come up with two policy papers which are surprisingly similar in aims and strategies! This looks like a case where the two countries are united over the issue. They indeed are if one looks at their actions without a context only. Introduce the context of the recent conflict and a different picture emerges with deeper insight into the two different routes leading to the same position. Without context, meanings lose their life and significance and conclusions can be nonsensical. Also, in a world of actors that consist of states, non states institutions, the action can have different meanings in different context. This can be corroborated by another example: A big MNC's chief says, "Cyber espionage has cost us $ 1 billion in the last five years. It is indeed an astronomical loss and is a big threat." This is mere statement in which a company's boss is expressing concern about the problem of cyber espionage and the amount of loss worries him. But the context is missing and so the import of the statement can be only a wild guess. On the other hand, if it is known that the statement was addressed to a government machinery of the MNC"s home country in a policy making forum, then things become clearer. Then the use of the phrase 'big threat' is no more an expression of concern of a corporate man who thinks about his balance sheet only. In fact, it is an indication, a gesture to the policy makers to act fast. The urgency becomes visible with the introduction of context. Also, other details like the commercial power of the company and the position held by the person speaking in his country also make context more complete.

1.10.5 Analysis of Icons and Pictures

This aspect of the data has usually been ignored in the literature. In fact, the cyberspace governance has been studied with very limited sources. Symbols, icons and pictures have been the missing part in the whole analyses. This has to be attributed to what has already been mentioned about 'the acceptable areas of study' and 'acceptable actors in cyberspace governance'. It has been found that iconic data has been largely excluded owning to its absence in the sources like reports, speeches and policy documents. But umpteen numbers of such symbols exist in internet at various sites that have their own take on cyberspace. The analysis of these icons is more or less similar to other textual sources. However, there is some specificity that has been taken into account. Pictures carry message only when their historical, ideological and cultural import is understood. In this case, icons and pictures complete with sometimes a colour combination along with events and audience/target, provide the context. Many platforms propagating a state control free cyberspace have made subtle use of such schemes. They do not make sense unless one looks at the nature of discourse the issue is subjected to. Therefore, the analysis is done with the help interdisciplinary insight. As opposed to the other textual data, these have to be looked for in online sources and their messages about cyberspace have to be decoded in the context of times and events that they are taking about. The rest is usual content analysis. The most common sources for these data are the websites of organizations that make up popular and not so popular sites that work on different areas of internet.

1.10.6 Interviews

Interviews form an important part of this study. Interviews have been sourced both through e-mail correspondence and through face-to-face meetings. They have helped in correcting many notions. Therefore, interviews have helped in reviewing the existing understanding about Russia. The interviews have allowed the interviewer to gain insight on issues that the country is grappling with at an international level as well as domestic level.

1.11. Chapterisation Scheme of the Study

The chapters have been made after taking into consideration two things. There are a number of issues relevant to cyberspace governance. These have affected most countries. Russia's approach to these will be in context of these. On the basis of this, five chapters have been written. The first chapter titled *'Introduction'* presents the research design of the work along with presentation of key framework/ assumptions that study makes regarding certain concepts. Chapter number two has been titled as *'Cyberspace Governance: Issues and State Practices'*. This is the chapter that discusses issues in participation of state and non- state actors in cyberspace that are the direct result of innovations and how their participation has given birth to several practices. Since many developments have taken place on this front in the last one decade; the chapter has tried to include as many changes as are relevant to the topic. Cyber security, militarization of cyberspace, Information industry, e-commerce, cyber laws, cyber policing, surveillance, censorship, cyber legal practices, copyrights, open access, network neutrality, localization of data, splintering of Internet, international governance of cyberspace, and role of ICANN are all topics that are dealt with to see various models of governance, the emerging trends and the practices of state.

Chapter 3 titled *'Domestic Factors in Cyberspace Scenario in Russia'* explains country's domestic factors that have influenced its stance on regulation of cyberspace. These factors have gained prominence lately and so carry even greater significance. The fourth chapter titled *'Russian Approaches to Cyberspace Governance Issues'* helps in understanding the country's approach or set of approaches to various problems of cyberspace governance. The country has formed its understanding on the issue and like any other state it too is experiencing churning on this issue with several voices coming up on myriad topics. Russian approach however does not mean just surveillance and censorship. The set of approaches span a wide range of issues from online piracy, copyrights to the laws against online sexual crimes. Finally, Chapter 5 called *Conclusion* puts the findings of the all the chapters with observations on the nature of Russian participation in the discourse on cyberspace governance. This concluding chapter also throws light on the latest developments in the globe as well in Russia which carry relevance for the future evolution of the discourse.

2.1 Introduction

The cyber landscape is changing rapidly for the last ten years. The changes are in several spheres of politics, economics, society, security, business, commerce and industries. These changes have revolutionized all these spheres. For states, the novelty is that cyberspace is not the usual sphere to which they can easily extend their taxation rules, political sovereignty and moralizing architecture. In other words, cyberspace defies their old logic. Therefore, the biggest challenge for countries is governance of cyberspace. The changes have been disruptive. This disruption has been caused by innovations that are changing the way wars are fought, understood, opinions expressed, theft committed, state secrets stolen or a nation is destabilized. It has made several resources freely accessible. Human-machine interface has made this possible because without a human need, such innovations would not be invented nor would spread easily. However, disruptive innovations bring issues with them and existing institutions need to adapt to them. Therefore, governance of cyberspace requires states to grapple with a number of issues brought by the disruptive technology. The first issue discussed here is militarization of cyberspace. It is a direct byproduct of inventions and improvisation of cyberspace to suit military needs. There is now new kind of threat: cyber security threat. There is a new mode of warfare: cyberwarfare. It has also brought into the open the need to have new definitions of peace, a peace that holds meaning in cyberspace. There is also a need to rethink the meaning of conflict. The first section deals with these questions.

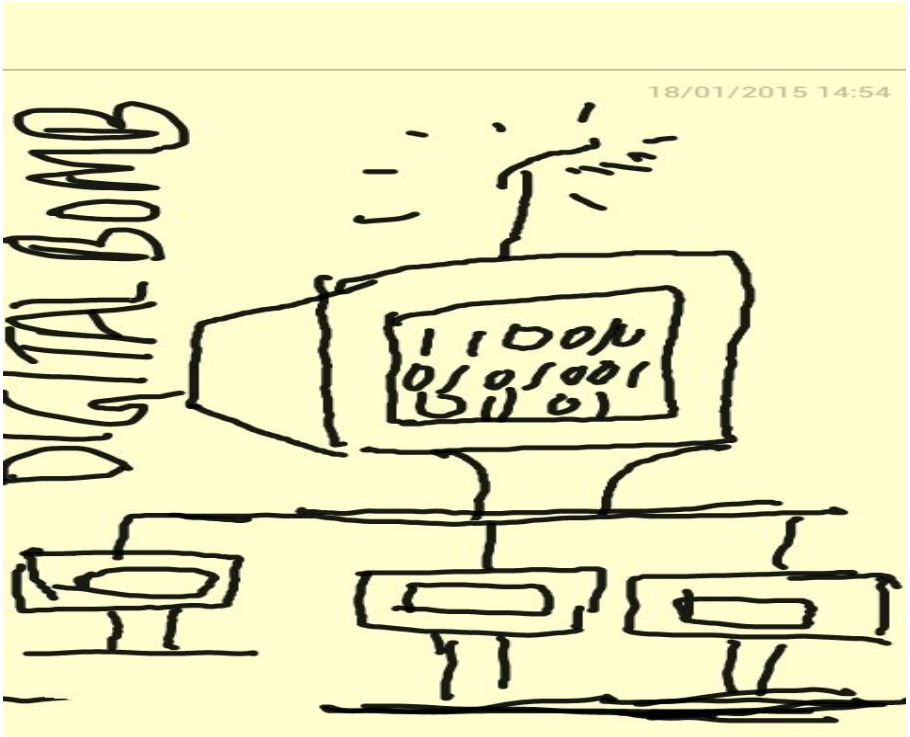
The second set of issues is cyberspace and state practices that curb freedom of citizens like blocking sites, instituting laws to prevent people from reading/ watching certain type of content, penalizing people for expressing a certain opinion, keeping tab on citizens through use of surveillance technology. This is followed by analysis of problems in role of cyberspace as a free resource. This includes issues of copyright violations, attempts by states to make laws on them; opposition by some people to the idea of restricting cyberspace in the name of copyright protection. Net Neutrality has been discussed too within this context.

Finally, two models of cyberspace governance have been discussed: Multistakholder Model and State led regulatory approach.

2.2. Militarisation of Cyberspace

Below is an illustration through cartoon indicating that innovation has made it possible to cause a sort of blast in a highly interconnected system.

Figure 2.1



When NASDAQ[8] in 2010 was affected by some intrusion by a malware that was detected as espionage and disruptive malware, the event was called ‘the placing of digital bomb’. It’s being called so is an instance of militarization of cyberspace. Militarisation of cyberspace is defined by this study as the transformation of cyberspace into a site of conflict that has known or unknown opponents. This has happened as a result of improvisation by states to suit their security and military needs. In this direction, USA has taken a lead. It formally set up a Cyber

[8] NASDAQ (acronym for National Association for Securities Dealers Automated Quotations) is an American stock exchange which is second largest stock exchange in USA and in world by size of market capitalization and volumes traded.

Command in 2010 to tackle threatening cyber activities; the country had already formed a well defined threat perception even if it meant dealing with enemies in the dark. In 2006, USA had already formed idea of the extent of threat that cyberspace posed to the various facets of life of the country. It did not wait and made cyberspace security a major task of the US Air Force. US Air Force Cyberspace Task Force Director Dr. LaniKass at the time laid out the tentative ideas by emphasizing the cyber domain and the potential harm that the country could face because of the connectivity that it provides. He said: “Our life has become totally bounded, dependent on cyberspace. Therefore, the importance of that domain is not only for how we fight but also our way of life.”(Daly 2006). Later in 2009, US Deputy Defense Secretary William J.Lynn III described how the ability to destroy was once a ‘province of nations’ but had now been acquired by smaller actors like terrorist groups, industrial spies, hackers and organized crime groups. The urgency was patent in his statement: “This is not some future threat. The cyber threat is here today; it is here now” (Kruzel 2009). US President Obama also laid out in his statement the widespread cyberspace and how it covered every facet of life. He called cyberspace and the threats emanating from it ‘real’.

USA had conceived the plan of Cyber Command way back in 2006. That year did not see either the Estonia cyber meltdown due to Russian hackers nor did the world witness the Russia-Georgia cyber escalation. Both are now popular historical events that took place after US conception. But when US President sent the message on US Cyber Command, the Russia-Georgia cyber escalation, use of VoIP by terrorists in Mumbai attacks on the Taj Hotel and cyber threats from groups like Al-Qaeda were very much part of the speech (Remarks by President Obama on securing nation’s cyber infrastructure, May 29, 2009). Out of all the attacks, the Russian offensive against Georgia became very significant. The conflict had been triggered by the now breakaway regions of South Ossetia and Abkhazia which has significant Russian ethnic population. The normal military confrontation assumed one more aspect which was the cyber offensive. When Russian tanks were rolling into Georgia, a cyber offensive was launched by several small non-state actors like hackers. The offensive included defacing of sites, DDoS attacks and PSYOPS that did more harm than imagined. The foreign ministry and President’s website became inaccessible and phone calls were affected leading to communication paralysis. A year before the Georgian crisis, Russian hackers had brought down the economic networks in Estonia to a halt thanks to the rise of anti-Russia sentiments among Estonians over a Soviet era statue. After this, US quickly implemented the idea of having a cyber command. The threat perception that US had formed was actually being played out in the laboratory in the borders of Russia. Every turn of event related to the crisis only confirmed what it had deliberated upon.

In cyberspace militarization, US has sought to act a leader and many have followed and responded. The establishment of US Cyber Command is just one of those actions. But the way its spread has been done. When US Vice-President spoke at the 45th Munich Conference on Security Policy which was a NATO gathering, he said: “Our alliance must be better equipped to help stop the spread of the world’s most dangerous weapons to tackle terrorism and cyber security, to expand the writ of energy security and to act in and out of area effectively.”(Vice-President’s Remarks at the 45th Munich Conference on Security Policy 2009) The fact that it was a NATO gathering cannot be missed. The audience countries are all US allies or rather the followers. Emphasizing cyber security at a larger gathering of allies gives a cue to the latter that military aspect of cyberspace needs to be developed. Much of what US wished to convey has already occurred by now. If Pentagon’s cyber command budget has increased to a record $447 million, then NATO states have also simultaneously increased their cyber security spending (Apps 2014).

It is not just the NATO countries that have responded in that fashion. Several member states of Organisation of American States have followed their own tailor made approaches for handling the cyber security threats. Government of Argentina has established the National office of Information through which Ar-CERT (Argentina Computer Emergency Response Team) was created way back in 2005. In 2013, the country was well on the way to its full National Cyber Security Policy. Columbia led an ‘Operation Unmask’, which was multinational operation to bust a ring of transnational cybercriminals and some hacktivists. The other countries who participated in it were Argentina, Chile, and Spain. This operation was conducted nearly a year after the country in question had adopted a highly muscular and militarized approach to the cyber security problems. It had set up in 2011 Centro Ciberne̋tico Policial(CCP) which translates into Police Cyber Center. It also set up Joint Cyber Command which is a military unit responding to attacks against the nation’s assets. Jamaica also oversaw creation of its National Cybersecurity Task Force in 2012. Mexican government has also formed National Specialised Cyber Incident Response Team. In 2013, Panama also joined the group of countries who have a formal National Strategy for Cyber Security by adopting a national strategy for the same (Trend Micro 2013: 20-22).

Apart from these Latin American and South American countries, the other state actors with prominent policies on cyber security include China. Incumbent Chinese President Xi Jinping has taken the militarization to an entirely new level. He recently took charge of a government body on cyber security and vowed to make China a ‘cyber power’. By pronouncing its ambition, it has taken the militarization discourse to a level which sees race among nations to outsmart each other in cyber defense and offense. ‘Power’ is a loaded term in the context of earlier actions of USA. In the light of USA’s vast and deep reach in surveillance exposed by Edward Snowden, the statement reflects country’s will to gear itself up for a big role in militarized cyberspace. China moves not only in the footstep of USA but also seeks to outdo the latter by openly calling for making itself a cyber power.

2.2.1. Dealing with a new warfare, a new notion of conflict and peace

Cyber war as a concept has been discussed by Martin Libicki. While describing the nature of this new warfare, he says that it is a warfare which lacks the power to destroy one or more parties to a conflict and it takes some options of attacks off the table because the war lies below the level where either side has the reason to escalate the conflict. He also explains that it is not possible to have a formal peace agreement because neither the perpetrator nor the victim would actually admit to it. Even if some kind of informal peace agreement happens, it is problematic because it is difficult to monitor such peace pacts (Libicki 2009a). The US-China conflicts that have happened in cyberspace lately reflect the peculiar nature of cyberwar. It is easy to define neither war nor peace when events are taking place in cyberspace. How can one decide that cyber conflict is is going on or peace is being maintained? According to United States, China has been behind increasing number of attacks on its cyber systems. Tom Donilon publicly raised the issue of Chinese hand behind such attacks early in 2013. Not only did he raise the seriousness of the problem but also called China to come clean on the problem and to crack down on the hackers who were behind the attacks. At the same time, he made it a point to tell China that the increasing attempts to attack in this way was not "acceptable norms of behaviour of cyberspace" He also said that until some time back USA had avoided naming China publicly although President Obama had raised the issues privately with Chinese authorities (Landler & Sanger 2013). China denied its role with its Foreign Ministry spokesman saying: "China has repeatedly said that we resolutely oppose all forms of hacker attacks. We are willing to carry out an even-tempered and constructive dialogue with the US on the issue of Internet Security. But we are firmly opposed to any groundless accusations and speculations, since they will only damage the cooperation efforts and atmosphere between the two sides to strengthen dialogue and cooperation."(Sanger 2013). The actions of both the countries are part of the militarized approach to cyberspace.

The talks between US and China that began more than a year ago are along lines of other military issues. The manner of US finger pointing and later setting up of US-China Working Group on Cyber Security in April of 2013 was a way to defuse an escalating problem. The group met later in the year to discuss the "international law and norms in cyberspace"(BBC News China, July 9 2013). These talks through the working group were however discontinued after the Snowden episode. The Snowden revelations showed that USA's NSA had hacked the network infrastructure at universities in China and Hong Kong. China was also miffed by the charging of five Chinese military officers with hacking American firms (Kang Lim & Roche 2014, the Reuters). The talks however have not been completely disrupted as much has happened informally outside the Cyber working Group (CWG) that the two countries had set up. During these talks outside the framework of CWG, US expressed its views to Chinese representatives on the emerging cyber threats. USA has called it cooperation on cyber security. These processes do bear some semblance to traditional measures that are adopted by countries to defuse tensions. However, it is still not clear whether cyberspace can be subject to the kinds of processes and laws that have governed war and peace so far in other old methods of war. According to Rex Hughes (2009:110), the national power projection in cyberspace makes the digital arms race imminent. Therefore, the cyberspace arms race and the future interstate competition are the central issues today. There is no consensus on the application of Law of Armed Conflict to the cyber war because of the loose definition of the phenomenon. The problem however is that a 'complete hands off policy' that does not assume cyber war as war at all may cause disruptions to the cross border transactions as the realm of cyberspace has no clarity of borders. This area in the militarized discourse has significance for how cyberspace governance is readied for fighting small cyber security threats and also full blown cyber offensive that throws the whole cyberspace into haywire. In this regard, two questions have come up that are related to application of International Humanitarian Law (IHL) to the cyber conflict. Since, cyberspace infrastructure is most widely spread and is utilized by civilians as well as military, any belligerent action of a state that brings down the information network of a country, can have impact on the civilian usage during such offensive. How countries come together on this point of cyberspace governance requires consensus on two contentious points. First is the Principle of Distinction under the Additional Protocol I of the Geneva Convention and the second problematic question is about the Neutrality Principle under Hague Convention. Both are discussed below

2.2.1.1 Principle of Distinction

The Principle of Distinction under International Humanitarian Law actually means that the belligerent state will distinguish between civilians and military targets. The civilians are afforded several protections under the Additional Protocol under the Geneva Convention of August 12, 1949. Article 51 of the Protocol provides for protection to civilians during armed conflict. The clauses: (1), (2) and (3) deal with provisions of protection of civilians. It is however the clause 4 which has the potential to trouble any application of IHL to the cyber war. It is because the clause defines 'indiscriminate attacks' and prohibits them. Indiscriminate attacks are those that (a) Are not directed at a specific military objective. (b) Employs a method of combat that cannot specifically target a military target. (c) Employs methods that cannot distinguish between the military and civilian objects (International Committee of the Red Cross website).

Jeffrey Kelsey argues that IHL needs to evolve fast to accommodate cyber warfare because the nature of cyber warfare is complex. Cyber war can involve targeting defense installations, centralized defense communication network, civilian facilities like hospitals, transportation, power plants, and telecommunication and media outlets. Also, the attacks can be precise and widespread enough to cover civilian installations or ones that affect civilian life. Apart from this, cyber attacks can be lethal as well non lethal. Due to the last point, a belligerent may frequently launch cyber offensive and cause damage to the civilian installations. If IHL does not evolve to include this nature of the warfare, then more indiscriminate targeting of civilians is to be expected than what was seen during cyber attacks on Estonia from Russian hackers in 2007 (Kelsey 2008: 1434-1436). Given the nature of definition of indiscriminate attack, it is actually difficult to expand the reach of IHL to cyber attacks. In this context, Robert Geiβ says that if for instance downing the network in a university is defined under IHL as not amounting to attacking civilians or civilian infrastructure, then the belligerent may be tempted to raise the threshold of the attack. It may actually result in raise in the nature of targeting of civilians. He however concedes that IHL can still accommodate the types of cyber attacks that are likely to result in severe accidents like release of radioactive gases or liquid and breaking of a dam that can cause flood (Geiβ 2010: 372-373). Therefore, presently there are both theoretical and practical problems in extending the Principle of Distinction to a situation of cyber war. However, the moves made by USA and China indicate that the next few steps in the area of cyberspace governance may involve better understanding about cyber war that countries are engaging in without owning up responsibility.

2.2.1.2 Principle of Neutrality

Under the Article 1 of 1907 Hague Convention No. V, the territory of a neutral State is inviolable which means that warring parties are prohibited to commit any act of hostility whatsoever on such territory. A neutral state is described as one which has taken formal position of not participating in an armed conflict or which does not want to get involved. The neutral state is granted certain rights and duties. The rights include right to stand apart and not be attacked and duties include non-participation and impartiality. Presently, international law of neutrality during armed conflict says that neutral space can comprise the national territory of the neutral state, its territorial waters and its national air space (ICRC website).

Kelsey argues that cyber war allows a belligerent state to take advantage of cyberspace. An information packet carrying a malicious code can travel through the information node of the apparently neutral state to wreak havoc on the ultimate target. But this may prompt the target to conclude that the neutral state is also involved in the attack. This may invite reprisals from the target state and ultimately suck into the conflict the earlier neutral state. This is of course violation of Principle of neutrality if it is assumed that the situation is one of cyber war and the neutral state is indeed a neutral state. Also, the cyberspace may tempt a belligerent state to engage in violation of neutrality of another state in order to reduce risks for itself. If the country it is targeting looks averse to retaliating against a neutral state in the event of its information node being used, then the attacking state may be more inclined to violate a neutral information space. Therefore, the scholar has argued that it is high time that IHL gets to change itself through custom and state practices to encourage the use of cyber weapons in some situations and to provide better guidance in the conduct of such operations. He has also suggested the broadening of the definition of neutrality to accommodate cyber weapons and encourage their use over other conventional means of war.

It seems in the light of the present provisions in the international law of neutrality that it is not possible to even define what would amount to violation of neutrality because neutral space has not defined to include the cyberspace. Cyberspace presently has no borders. So it is difficult to define what all would come under a country’s share of cyberspace. Secondly, Kelsey’s suggestions are based on the assumption of clarity regarding who is belligerent and who is targeted. Presently, countries do not even own up the responsibility for the attacks. Even tacit acceptance is not made. The victim countries have remained largely mum on the attacks. It is only recently that USA has publicly named China as the one who has been suspect behind spate in cyber intrusions. Perhaps it is the first attempt to move towards a kind of discourse which accommodates cyber weapons and warfare methods. It is therefore a kind of strengthening of militarization cyberspace which is now no more in the realms of ideas and symbols. Going back to the situation of cricket commentary, the countries by attempting to co-opt cyberspace in the militarized realm are trying to make sense of the cyberspace. Negotiations with suspect country and talks on cyber security allow both countries to demarcate things that can be controlled by them. However, such actions are presently confined to few players only. Russia too has been in the news for the show of aggression but like China, it too has not come clean on this. It does not actually make sense to own up. What will be benefit of cyberspace if one has to come clean on every action of dispersed actors in one’s territory? It remains to be seen whether the US-China model of negotiations is extended to other countries. USA and China have led the mechanism which is for bilateral benefits. Any kind of multilateral effort is likely to take the militarization to a new level where the cyberspace will be fully co-opted by the age old language. Countries then would have read the cyberspace activities in language of bellicose that they have been using. It is strange that when cyberspace is regarded as the space that has provided so many new things to the world, it gets interpreted into bellicose the way commentator interprets the cricket scene with the knowledge that he already possesses about the activities in the field.

2.3.Practices that curb Internet Freedom

2.3.1 Content Regulation

When the National Security Agency (NSA) of United States was found to be conducting a widespread online surveillance across several nations, many countries were shocked to find that such a wide program could even exist. In 2015, Raif Badawi, the online civil liberties activist in Saudi Araba was lashed after getting sentence of 1000 lashes, a hefty fine and ten years prison term, and people squirmed. Both the events show that cyberspace is not immune from the powers of state nor is the limit of freedom in cyberspace a settled fact. Usually, states do not put a gargantuan network to track their citizens. Most states actually do what cyberspace has afforded them and that is using technology to keep things ‘controlled’. There are always pieces of information that are not palatable to the interests of the ruling regime or to even the predominant cultural or religious sentiments of the dominant community. These pieces of information can be made simply inaccessible or the routes to reach them made too slow to be reached in short time. People will therefore be following things in short time that are easily accessible. In cases where such a thing is not deemed publicly desirable, surveillance programmes are run. The surveillance enables the surfing behavior of people to be revealed to the select few in security agencies. If a government wants to reduce the spread of undesirable news or facts in a region, it can simply resort to bandwidth throttling to reduce the speed of internet. Bandwidth throttling involves putting limits on the amount of bandwidth that a person can use. Bandwidth throttling is one of the ways to filter the data.

An underlying assumption of these governmental practices is that since people will see only what is shown to them, so it is better to ensure that they see ‘desirable things’. The definition of desirable of course varies across countries, cultures and continents. For instance, Australia moved towards blocking pornographic and online gambling sites because it deemed them ‘inappropriate material’. Senator Stephen, who was Telecommunications Minister under the previous Labour government in Australia took the step of making it mandatory for all internet service providers to provide ‘clean feeds’ or ISP filtering to houses and schools. This included making all the data supplied free from all pornographic and inappropriate material. X-rated pornographic material, casino style gambling and certain forms of hate speeches and R rated computer games are illegal online in the country which means that they are considered inappropriate (Riley 2007). There have been several kinds of opposition to it. ISPs argued at the time that blanket content filtering would cripple the speed of the Internet. Civil libertarians organizations like Electronic Frontier Association have also warned that filtering could lead blanket censorship of drugs, political dissidence, information on euthanasia and other legal forms of freedoms and even legitimate material could be blocked. Giving such an instance, they argued that there had been an instance in which legitimate topics such as gun control and breast feeding were blocked (Hendry & Pauli 2008). The Australian Government’s position of course was stated by the Senator who said: “Labour (Party) makes no apologies to those that argue that any regulation of the internet is like going down the Chinese road. If people equate freedom of speech with watching child pornography, the Rudd-Labor Government is going to disagree. There are people who are going to make all sorts of standards about the impact on the internet speed. The internet is not going to a halt in the UK, it hasn't ground to a halt in Scandinavian countries and it's not grinding the internet to a halt in Europe."(ABC News, December 31, 2007). Therefore in the Australian discourse on filtering, it is the 'care and control' that becomes dominant.

However, this is not the case in all the countries. In Islamic states that have autocratic governments, the controls imposed depend on more than just morality. Two kinds of contents are viewed suspiciously and with scorn: one is any tendency of freedom of expression that questions the existing regime and the other is material that is regarded as religiously immoral. For instance, Saudi Arabia redoubled its crackdown on online political activism after the breakout of Arab Spring events fearing serious rebellion in its own territory. The authorities almost freaked out. The reaction to this has been the arrests of several online activists. Apart from this, the country also engages in faith based censorship of online material. There is a state sponsored institutionalized operation called Hisbah which is the Committee for the Promotion of Virtue and Prevention of Vice, a kind of religious police that enforces Sharia law. This group has put up a study titled on its website titled "The Moral Vice of the Internet and How to Practise Hisbah. The study seeks to 'educate the public about the danger and the potential threat of immoral websites, provide religious advice to the operators of such websites, eliminate the wrong kinds of websites and increase the beneficial content. This kind of censorship has been extended to the social networking sites. Other Islamic countries have also engaged in similar faith based censorship. These include Sudan, Egypt and Nigeria (Noman 2011: 4-5). According to a Google research, out of top ten online pornography watchers, six were Muslim countries which included Pakistan at the top, Egypt at the second and Iran, Morocco, Saudi Arabia and Turkey at numbers four, five, seven and eight respectively. The reason could be the ban on sale of pornographic material in Arab countries except Lebanon and Turkey (Desk 2015). No wonder, then, the governments are sensitive about the material circulating online.

These are not the only reasons for the wariness among these countries. There has been an argument that apart from the pornographic material, there are several other websites that are destroying the base of the culture of the country, morals of the society and most importantly threatening Islam. Presence of evangelical websites has been noted in such arguments. According to them, these websites need to be regulated or censored because they are making efforts to Christianize the people (Noman 2011:7). In times when countries have mutual suspicions due to religions and sectarian tensions in the Islamic world, religion becomes a turf to be defended at any cost. Therefore, there is oversensitivity to the presence of websites like Internet Evangelical Coalition whose stated purpose is to utilize web for reaching out to both believers and non-believers. Started by Billy Graham Center in Illinois, USA, this has the open aim to “connect resources and partners for extensive and effective Internet evangelism” (Huston 2006). If one also looks at the conflicts in which Christian populations have been targeted by extremist groups in several conflict zones in Muslim countries, one is able to connect the urge of some countries to speak out against these websites that have become symbol of threat to the survival to their religion. The countries also look warily at the blogs that encourage conversation between participants on the topics of faith because they stimulate questions that may challenge the status quo though that may not be the actual purpose of such blogs. Therefore, the dominant things in the filtering and content control practices of these countries are the religion and regime (the two Rs). These two also happen to be largely regulated by governmental bodies largely in the said countries. Therefore, cyberspace discourse is sought to be controlled by the states. But governments are not conducting a monologue on the stage. Much of their actions have been either reactions or preemptive actions to thwart the online activism which has been flourishing with the advent of social media. Social media fuelled by Facebook, Instagram, Twitter and several other Internet Relay Chat platforms have fuelled congregations in virtual space which enables one to reach millions within seconds. These platforms present ordinary people to register very effective protests.

Figure:2.2

Source: www.patheos.com

Saudi Arabia, for instance, has very strict and rather archaic driving rules that permit only men to drive. Women are not allowed to do so under any circumstances. The logic given by the conservatives in the kingdom is that driving right would encourage women to be promiscuous (Griffith 2011). However, several women took upon themselves to protest by driving and making sure that their government gets to see them behind the steering wheel. The photo given above is one of the photos that the protestors circulated in the media to ensure the success of their protests. In this, cyberspace played a crucial role in spreading the message to the world and of course to the government they wished to convey their message to. Saudi government's reaction was one of warning to the other potential protesters to desist from violating rules and posting them online.

2.3.2 Surveillance Exports

There is strong urge to keep citizens under tab and to filter the online content. The reasons vary. But the governments use all the possible means to employ the best technologies. There are a number of companies that offers the required and any future talk on cyberspace governance has to reckon with this aspect because these companies form important part of the information technology sector. Intel, which is well known name in the software industry sells a product called Smartfilter. The latter is a product of Secure Computing, a company that was acquired by Intel as part of McAfee, another well known name in the industry. The product Smartfilter has traditionally been used by Tunisia for identifying sites that will be censored. The country has also been using Deep Packet Inspection (DPI) for which the common vendors have been European and American companies like Blue Coat Systems, NetApp and Ultimaco. Multiple surveillance infrastructures has also been created and maintained with the services and products of Nokia Siemens Networks, ETI (which is a subsidiary of BAE Systems), Blue Coat Systems, NetApp, Ultimaco and Trovicor. The French Internet Service provider Wanadoo has been one of the important technical consultants for the Tunisian system of censorship and control. Egypt, which experienced Arab Spring events and changes brought by them also has surveillance infrastructure which has been maintained by an American company called Narus. Telecom Egypt and Narus entered into an agreement for the surveillance technology for which a local Egyptian consulting firm, Giza Systems acted as mediator. Giza Systems has connections with several other vendors of Deep Packet Inspection vendors and was responsible for installation of Narus technology in the networks of Telecom Egypt.

According to Ben Wagner, these kinds of exports have implications for human rights violations in the buyer countries because although these technologies are of dual use, they are typically used for the single purpose: the one that limits individual human rights (Wagner 2012: 7-11). The issue however is not simple and it is difficult to impose blanket ban on exports of such technologies because these are dual use technologies that are used for securing the systems by governments and non-governmental organizations and for several genuine national security purposes (Cohn, *et al* 2012). Also, role of developed western countries that happen to be their exporters make things difficult. UK has been an enthusiastic seller in the unregulated market of the surveillance technologies. It has been exporting two powerful technologies in the international market including IMSI catcher and Trojan horse softwares. IMSI catcher technology masquerades as normal mobile phone masts and can identify phone users and malwares. It allows its operator to control the target computer without the interception getting detected. The second technology Trojan horse is used by hackers to activate the microphone and camera on another person's phone. Apart from this, the country has also exported optical cyber solutions that can tap submarine cable landing stations and capture mass surveillance of entire population. Presently, Privacy International, that keeps track of these exports from human rights angle, says that UK's customers include countries like Syria, Iran, Yemen and Bahrain (Doward and Lewis 2012).

The other major exporter is Germany, the country which is regarded as one of the engines that runs the world economy. In the wake of sensitivities about surveillance, a British-German company called Gamma International came under the scanner of parliamentary inquiry in Germany. It is known for selling the infamous FinFisher surveillance toolset. This is a toolset that can target unsuspecting targets. Once a seemingly safe link or e-mail is clicked, the software is downloaded and once it is installed, the toolkit allows its user to access even encrypted information. With the help of these, keystrokes can be logged and Skype conversations can be recorded. The German parliamentary inquiry has found that the exports were made to a long list of countries that included an assorted mix of countries. Apart from the already mentioned buyers from Gulf and northern Africa, the list also included Albania, Argentina, Chile, India, Indonesia, Kosovo, Qatar, Kuwait, Lebanon, Norway, Russia, Switzerland, Singapore, Taiwan, Turkey and Turkmenistan (Wagner &Guarnieri 2014). Given the various kinds of political systems and regimes prevalent in these countries, it can be said that obsession with surveillance is not confined to just the Islamic countries with old entrenched autocrats and dictatorial tendencies. Although, names of Germany and UK have been doing rounds, it is United States that has a concentration of cyber security companies which are all flourishing with sale of similar technologies. According to an estimate, the cyber security market is highly competitive and fragmented but the top 20 companies in the market are mainly the US based IT and Defense companies. It includes names like Hewlett Packard Company, IBM, Intel and Lockheed Martin (PRNewswire). According to Richard Stiennon, the cyber security industry is likely to see boom thanks to the mistrust that countries and companies have. The boom is expected to take place in areas of technologies of encryption, certificate management, surveillance and authentication (Stiennon 2013). Dominance in the market and good prospects of the industry has even translated into increasing influence in the policymaking areas. For instance, since United States leads in the market and is often followed in these matters, the Cyber Security Industry Alliance called on the Federal Agencies and White House to increase the investment in cyber infrastructure to protect end users. The body had a long list of suggestions for the policy makers. It included dedicating an Assistant Secretary position in Homeland Security, quick ratification of Council of Europe's Convention on Cybercrime, encouraging information security governance in the private sector, closing strategic gap between government and private sector information security efforts and increase in R&D for cyber security (PRNewsire 2014).The muscle of US cyber security industry is therefore good enough to bring many policy level changes some of which are already visible with increased focus of countries on the cyber security.

It is important to see the implications of militarization for cyberspace governance. For governments, it may mean a separate department for handling cyber risks, security threats and for many others it may mean increased workload of intelligence agencies. It also means increased use of biometrics to keep database of details of all residents of the country. A security centric policy may also result from militarization as in case of India's Cyber Security policy unveiled in 2013. The objectives mentioned in the India's Cyber Security document unveiled by the Ministry of Communication and Information Technology in 2013 sets the objectives which are:

1. To create a secure cyber ecosystem in order to generate adequate trust and confidence in country's IT systems and transactions in cyberspace and enhance the adoption of IT on all sectors of the economy.
2. To create a framework which can enable compliance with global security standards and best practices in products, process, technology and people.
3. To strengthen regulatory framework for ensuring a secure cyberspace ecosystem.
4. To create a system that is 24x7 and can be put at the disposal of prediction, prevention and crisis management.
5. To set up National Critical Infrastructure Protection Centre and mandating security practices related to spheres of design, acquisition, development, use and operation of information resources.

6. To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.
7. To enable protection of information in stages of process, handling, storage and transit in order to safeguard the privacy of citizen’s data.

In order to meet above objectives, a system is required that can meet the diverse objectives provided in the policy. Although the document is not a military statement, it has the imprint of security language. The structures required to secure the aims in this case would enhance cyberspace governance that seeks to ‘secure’ the country’s systems. This means more investment on information systems and software that secure.

2.4 Cyberspace as Resource

2.4.1 Free Information and Ideas Vs the Copyright Regime

2.4.1.1. Publishing Industry’s grouse

It is not uncommon to find young researchers in several parts of the world to surf the Internet, looking for some books. But the books they are looking for are not the ones they will eventually pay for. They are the ones that are available for free download. The best books by the best names in the world of writing and research are available at several free libraries online which can be accessed even without signing in without passwords. From the perspective of a student or an avid reader, these online libraries or collections are like the ultimate support of cyberspace that comes to their rescue in times when books by top publishers cost several dollars. Cyberspace then becomes a zone for several people who access these sites. These sites improve access to the ocean of knowledge which would have been beyond their means in its absence. Library.nu previously called ebooksclub.org or gigapedia.com, was one such site that was popular for free download of books. This was not taken lightly by the well known names in the publishing industry. The strong and established players of the industry came together, to knock off such sites. The major contention of these publishing behemoths was that such sites were encouraging piracy and were doing immense harm to the copyrights and the valuable intellectual capital of the knowledge industry. They argued that sites like library.nu had links to millions of pirated e-books and were hosted on cyberlocker ifile.it with the help of which the sites had generated millions of euros in advertising. The site was also accused of linking to a large number of academic texts that were published under the most prominent names in the publishing industry such as Elsevier and Oxford University Press. Therefore, the players coordinated their moves and it resulted in coming together of German Publishers and Booksellers Association and International Publishers Association against the sites that were providing access to pirated material. The statement of these players was that they continued to stand up against organized 'copyright crime' (Robertson 2012). The publishing bodies hired Lausen Rechtsanwalte, a Germany based law firm that is known for tracking down and prosecuting copyright violations. The downloads of library.nu were apparently hosted by ifile.it which is under ownership of Ireland based company DF Hosting. Its web address appeared to be hosted in Ukraine even though the web address was registered in a small Pacific island (Losowsky 2012). The efforts made by publishing industry have come after a studied silence during which they observed the changes that cyberspace was bringing to their model of knowledge circulation. It is amply clear that cyberspace gives alternatives to the older system that relies on copyrights regime. Even after taking down of library.nu, there are many sites available that offer free download of e-books. The challenge posed by cyberspace to the publishing persists, causing them to brand the violations in virtual space as a 'criminal action'. It is either the bitterness of the industry that is trying to catch up with the change or it is the strategy to go whole hog against the new rivals.

2.4.1.2. Film, Music and Art Industry's Bitter Fight

Billions of people download movies, music, songs and several art works for free. The oldest grouse of the film, music and art industry since the dawn of file sharing sites has been that they are losing billions of dollars due to copyright infringements from the sharing of these files that have been downloaded for free. Hollywood producers and studios have the biggest grievance against a system that allows people to do so.

i. The isoHunt Vs MPAA Case

Motion Picture Association of America (MPAA) is a very important body in USA. It describes itself as "economic engine that brings new jobs and economic opportunities and compelling entertainment content to communities around the world". They claim to support 1.9 million workers (costume designers, make-up artists, stuntmen, set builders, writers, actors, accountants, special effects technicians, etc.). They also call themselves a body that is contributing $38 billion to around 330000 businesses annually and approximately $16 billion to US federal and state tax kitty (www.mpaa.org). In their own words, they represent creators and makers who bring entertainment. Given the number of Hollywood movies that are produced and the amount grossed by even not so good movies, their estimations are believable. They actually represent Hollywood's powerful film studios that have great stakes in movie making and a movie's earnings at the box office. Copyrights are sacred to MPAA as they believe that it is the copyright regime that has spurred creativity and its infringements affect the incomes of several artists. Recently they won the copyright battle against isoHunt Web Technologies. The problem arose due to some infringements by the Torrent method of download that became copyright battle with MPAA. isoHunt Web Technologies was founded by Gary Fung. It founded file sharing sites Torrentbox.com and Podtropolis.com through which music and films files were shared. Hollywood's famous studios Columbia, Disney, Paramount, TriStar, 20th Century Fox, Universal and Warner Bros. filed the suit in 2006 alleging that sites induced "untold number of users to illegally download and distribute MPAA members' pictures and television shows over BitTorrent peer- to- peer network (Miller 2013). The US Court of Appeals for the Ninth Circuit ruled in favour of MPAA upholding the argument provided by the latter. Along the lines of *Napster and Grokster* case[9], the court ruled that online music sharing services can be held

[9] Metro- Goldwyn-Mayer Studios Inc. v. Grokster Ltd. was a landmark case in the history of copyright cases. In 1999, a college student released Napster. Napster was a file sharing application in the Internet. The music fans found it extremely useful because it enabled trade in copyrighted music works. The music recording industry filed a suit in 2001, the judge ordered Napster to shut down. This case had hardly gone into oblivion when other start- up companies with Napster like applications but had innovated enough to avoid legal hassles of copyrighted violations. The innovation was major. Napster allowed users to browse each other's computers and share copyrighted music but the transactions were routed through Napster's own internal servers. The court judged the company responsible for violations because of internal servers. Now, the new companies Grokster and Stream Cast innovated by abandoning the centralized servers, allowing users to connect directly with each other. As expected the music and movie companies sued Grokster and Stream Cast in 2001 for providing file sharing service Morpheus and Kazaa. The technology companies supported the Grokster type companies and the defendants in this case for they believed that they were encouraging innovations. In 2003, a Federal judge ruled in favour of the defendants. Appeal was made by the aggrieved parties and the Ninth Circuit Court of Appeals upheld the earlier ruling. The case then went to the Supreme

responsible for copyright infringements if the services induce the uses that cause infringement. The court argued that isoHunt was guilty of contributory copyright infringement because it provided platform and encouraged the users to infringe protected works (Busch 2013). Gary Fung's response to the ruling was that his site only acted as a search service and was not hosting files like You Tube did but the court did not agree saying the site had torrent file tracker with the help of which users could find an uploaded file (Miller 2013).

ii. SOPA and PIPA :Cyberspace takes the protests to netizens

The events described above are reflections of the challenges that countries are expected to face in adjusting to new technologies that render old regimes of copyrights redundant and ill-equipped to deal with new age in which sharing is fast. Therefore, online copyrights are one of the most important cyberspace governance issues. Much of the action on this front is taking place in the west because the innovations are still taking place there largely. Also, the rich music and art industry behemoths are mostly in western capitals. A debate on this broke out when USA moved to introduce bills to protect copyrights in cyberspace. The uproar over the introduction brought out in the open the cleavages on the issue of online copyrights.

In year 2011, USA introduced two bills that were aimed at penalizing websites that threatened intellectual property and copyrights. Of course, some of the preceding events in which sites were found guilty of encouraging infringements of these rights were in the mind of the US lawmakers. Their actions can be attributed to the brouhaha created by the entertainment industry. The first bill that was introduced was in May, 2011 and it was popularly called PIPA which stood for Protection of Intellectual Property Act. The bill was introduced by Senator Patrick Leahy and others. Leahy commented that his proposals would permit law enforcement agencies to crack down on rogue websites dedicated to the sale of infringing or counterfeit goods". The bill called PIPA said that "an information

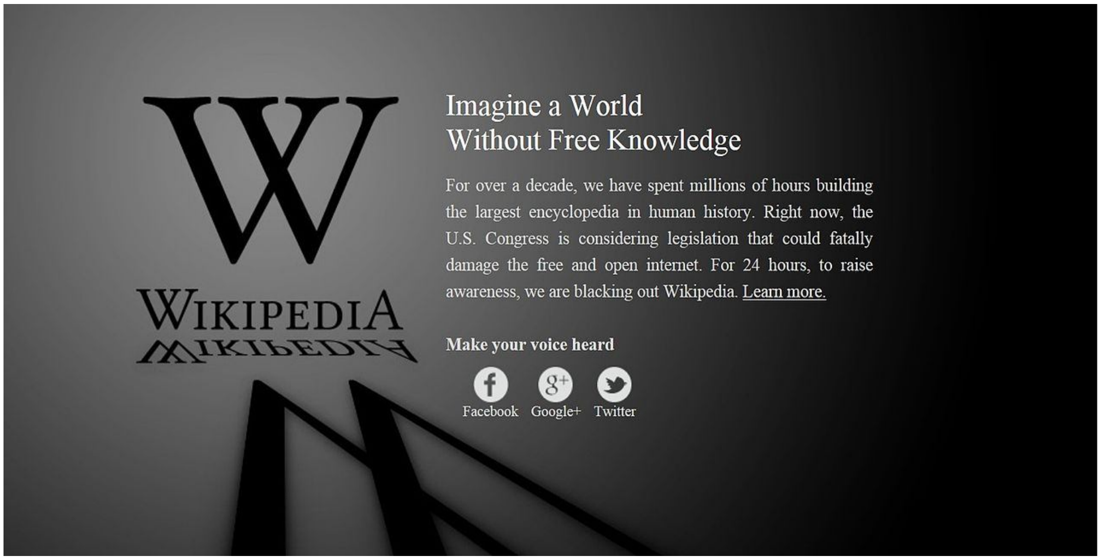
Court which is the final court of appeal in USA (McGuire 2005). In June 2005, the court unanimously held that Grokster could be sued for infringement for their activities prior to the date of the judgment. Grokster settled with the plaintiffs after this decision and the plaintiffs later filed motions for the liability of the remaining defendants, StreamCast and Sharman. Sharman reached a settlement. On September 27, 2006, StreamCast's liability case was heard and it was ruled that "plaintiff need prove only that the StreamCast distributed the product with the intent to encourage infringement (Wikipedia.org).

location tool shall take technically feasible and reasonable measures, as expeditiously as possible, to remove or disable access to the Internet site with the domain name set forth in the order". The information location tool was defined as directory, index, reference, pointer, or hypertext link. Due to the definition of the information tool, search engines like Google, Yahoo and several others were brought under the ambit. The move was backed by the movie studios and large copyright holders (McCullagh 2011). Then in the same in the month of October another bill was introduced. This one was named SOPA (Stop Online Piracy Act). This was introduced in the House of Representatives. SOPA had the provision that allowed Federal Bureau of Investigation to seek injunctions against sites that stole music, films, software and other intellectual property created by US firms. It also had provision that could hold third parties like payment processing and other partners responsible for piracy and counterfeiting. The bill was attacked by several tech giants and civil rights groups. Most importantly, the bill was aimed at 'criminalising' certain action that could be contributing to innovations. This was obvious from the statement from MPAA, one of the staunchest backers of the bill. Michael O' Leary, the executive vice-president of MPAA said that millions of people working in motion pictures and television shows deserved better than to see their work getting stolen from under them by the criminals out to make profits (Kang 2011).

The bill was criticized from several quarters. The reaction of Electronic Frontier Foundation after a short review of the bill was that it would do irreparable damage to the Internet. The organization wrote in its website: "This bill cannot be fixed. It must be killed" (Downes 2011). The initial reaction of the tech giants in Silicon Valley was muted but as ideas began to sink in, the protests became more vociferous and assertive. The most memorable were the online protests by an assorted mix of blackouts, symbolic protests, appeals to the Internet users to join the protests, call for protecting the Internet and its creativity. Google, Wikipedia, Mozilla, Reddit and several others actively participated on January 18, 2012 against SOPA and PIPA. It was well coordinated strike that had seventy five sites participating in it (www.sopastrike.com). It is important to discuss some of the important and memorable symbols of protests that veered the discourse of governance towards freedom and innovation for the latter two were the ideals which the sites claimed to be fighting for. In the next couple of pages are given some archival material which throw light on the same. The contrast in the perceptions of the participants is visible in the symbols. While lawmakers and movie studios considered certain actions criminal, an online and widely read encyclopedia like Wikipedia called SOPA and PIPA as “fatal to the free and open internet”(see the message in the darkened webpage of Wikipedia). Wikipedia is an online encyclopedia that changed the way encyclopedias worked and served. Right from its formal establishment in 2001 by Jimmy Wales and Larry Sanger, the online encyclopedia has emphasized the importance of a model that does not favour a centralized editing. Instead, the encyclopedia works on the basis of massively multiplayer editing. This undoubtedly promotes free sharing of knowledge. It is this principle of free sharing that Wikipedia was upholding when SOPA and PIPA were sought to be pushed by the US lawmakers. Had the bills been successfully introduced, passed and signed into law, a very big knowledge source like Wikipedia would have taken a hit in several areas as authors and editors source their facts and knowledge from several sources, many of them are copyrighted ones. The most famous symbol of Wikipedia became the darkened page saying “Imagine a World without Free Knowledge”. The message was a direct attack at attempts to kill an ecosystem that had fostered sharing and pooling in cyberspace and had spawned several Wikipedia type enterprises. Wikipedia in fact has become synonymous with ease with which curiosity about anything can be quenched with couple of clicks or touches on the smartphones. The protest therefore also became a symbol of the governance that they desired. They seem to want the bottom to top approach which is participatory and which is not inhibited with certain draconian measures in the copyrights.

Google which is now famous for coming up with thematic doodles invented a unique way to protest. The word Google in the search section was covered with a thick black band blacking out the whole word. The ubiquitous Google sign was not seen that day and immediately attracted attention. It actually meant that in a world muffled with copyrights, Google may vanish. Google’s Eric Schmidt called the SOPA and PIPA measures “draconian”(The Huffington Post, January 18, 2012). The protest symbol also read: “Tell Congress: Please Don’t Censor the Web!”(See second symbol below). Firefox also put up a page giving links to information about the legislation and exhorting people to join the protests. The Creative Commons also appealed to join Wikipedia and others in protests against SOPA and PIPA. It also provided a link to the book *The Power of Open* to emphasize the ethos that informed its enterprise. According to their description, Creative Commons is a Massachusetts based non-profit organization that ‘enables sharing and use of creativity and knowledge through free legal tools. It was founded in 2001. Their copyright licenses are easy-to-use, provide a simple and standardized way to give public permission to share and use their creative work on conditions of choice of one’s choice. They are not an alternative to copyright. Rather they work alongside copyrights. Creative Commons is suitable for publishing if one wants to give people the right to share one’s work. The NGO also maintains a huge pool of CC-licensed material available to the public (creativecommons.org/about). The participation of Creative Commons which is not antithetical to the copyrights carried huge significance because it gave a strong message that what the US Congress was trying to do was extreme and couldn’t be defended on the basis of even copyrights. Below are images of pages of some famous sites that took out online protest against the US Bills.

Figure 2.3



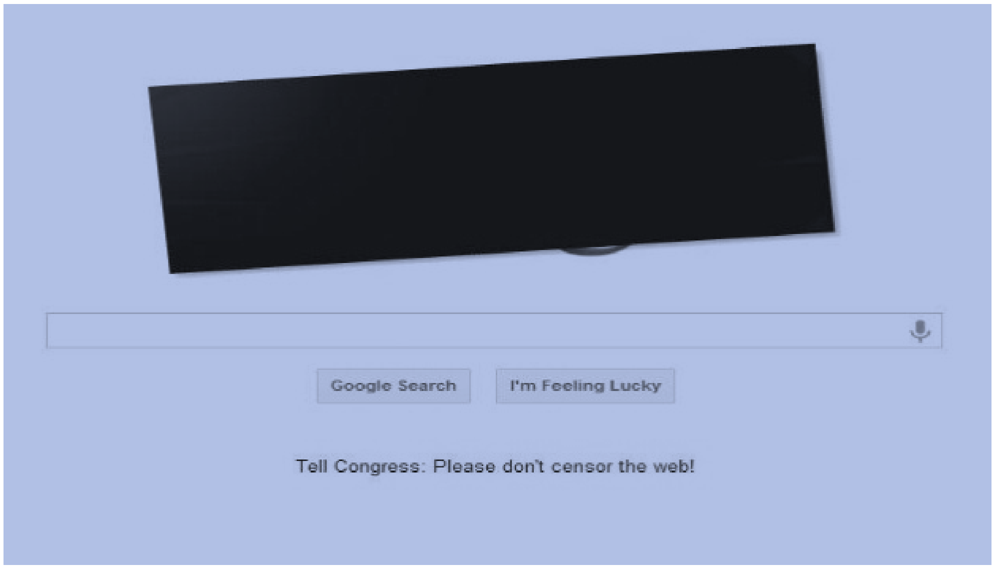
Imagine a World
Without Free Knowledge

For over a decade, we have spent millions of hours building the largest encyclopedia in human history. Right now, the U.S. Congress is considering legislation that could fatally damage the free and open internet. For 24 hours, to raise awareness, we are blacking out Wikipedia. Learn more.

Make your voice heard

Source: http://en.wikipedia.org/wiki/Protests_against_SOPA_and_PIPA

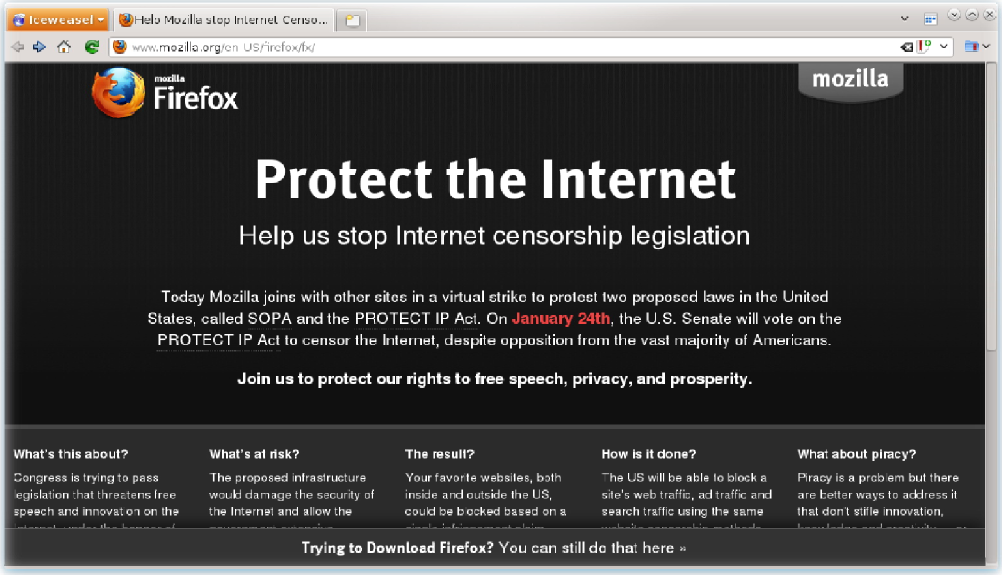
Figure: 2.4



Tell Congress: Please don't censor the web!

Source:http://en.wikipedia.org/wiki/Protests_against_SOPA_and_PIPA

Figure: 2.5


Iceweasel
Help Mozilla stop Internet Censo...
www.mozilla.org/en-US/firefox/fx/
mozilla
Firefox
mozilla

Protect the Internet

Help us stop Internet censorship legislation

Today Mozilla joins with other sites in a virtual strike to protest two proposed laws in the United States, called SOPA and the PROTECT IP Act. On January 24th, the U.S. Senate will vote on the PROTECT IP Act to censor the Internet, despite opposition from the vast majority of Americans.

Join us to protect our rights to free speech, privacy, and prosperity.

What's this about?
Congress is trying to pass legislation that threatens free speech and innovation on the

What's at risk?
The proposed infrastructure would damage the security of the Internet and allow the

The result?
Your favorite websites, both inside and outside the US, could be blocked based on a

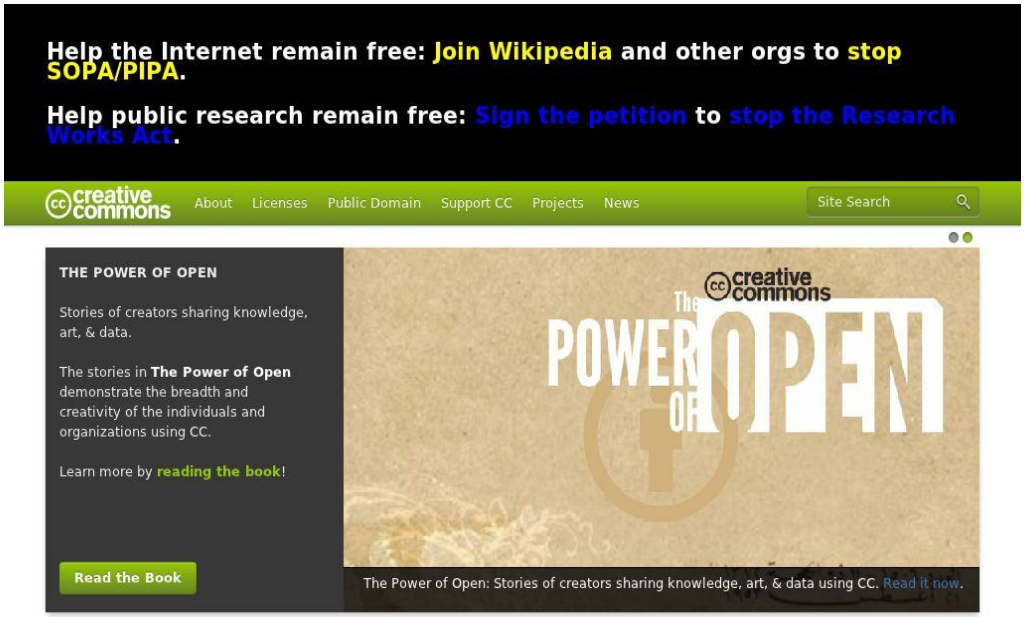
How is it done?
The US will be able to block a site's web traffic, ad traffic and search traffic using the same

What about piracy?
Piracy is a problem but there are better ways to address it that don't stifle innovation,

Trying to Download Firefox? You can still do that here »

Source:http://en.wikipedia.org/wiki/Protests_against_SOPA_and_PIPA

Figure: 2.6



Help the Internet remain free: Join Wikipedia and other orgs to stop SOPA/PIPA.

Help public research remain free: Sign the petition to stop the Research Works Act.

THE POWER OF OPEN

Stories of creators sharing knowledge, art, & data.

The stories in **The Power of Open** demonstrate the breadth and creativity of the individuals and organizations using CC.

Learn more by **reading the book**!

The Power of Open: Stories of creators sharing knowledge, art, & data using CC. Read it now.

Source:http://en.wikipedia.org/wiki/Protests_against_SOPA_and_PIPA

iii. Hacktivism against Control and Copyrights

The word ‘hacktivist’ is a combination of two words: hacker and activism. So, they are activists equipped with the technical skills of hacking who hack to defend certain values and ethos. Hacktivists are known to be connected to each other through various platforms and they perform actions to target organizations that seem to attack the values that they hold. Usually, hacktivists value freedom of speech, expression, freedom to share and transfer online. They are therefore the most extreme cyberlibertarians who detest any sign of control by the states. Copyright laws that apparently infringe on the right to express and access are their major targets. By virtue of this, the organizations that have been clamouring for protecting copyrights in cyberspace are their bête noire. These hacktivists have been watching the changes in the way states are encroaching upon areas that were earlier free. The most famous of their actions in recent times is Operation Payback which was a retribution for targeting sites that did not respond to copyright take down notices.[10]

iv. Operation Payback: Voice from the Cyber Anarchists

Controlling Piracy is like reining in cyber anarchists whom the states view suspiciously because they are bound by only their own ethics and not the laws that states institute for regulating human behaviour in cyberspace. The contrast with the mainstream understanding that gives primacy to laws, regulations for cyberspace was visible during Operation Payback. This operation was highly coordinated and involved targeting sites of big names in movie and recording industry around the world. Anonymous, the famous hacking organization, was the master of the cyber attacks which were part of the operation. It happened in 2010, the time when movie studios and recording industries were most noisy about threats to copyrights in cyberspace. So in September 2010, Warner Bros. studios, Universals, Sony and MGM became targets of DDoS attacks and were castigated for their stand. After attack on Warner Bros. Studios site, they released the statement in which they said that these companies are among organizations that had levied millions of dollars in damages against innocent people. They said that the attack was a response that would cause equivalent losses in downtime, corrupt data and focused distribution of their media. Referring to Pirate Bay against which these movie studios are known to speak, the operation organizers said that Pirate Bay was targeted by these studios because it could be made an easy scapegoat. The organizers also argued that these studios did not care about art or creativity or about the artists' rights. According to them, they understood only the language of money, so they were targeting where it hurt them the most: their wallets (Correns 2010).

The group also targeted CopyProtected.com, a site run by MPAA. The targeted site is used to give information on copy protection and DRM on DVD and Blu-ray movie discs. AliPlex Software, the anti-piracy company was also hit with DDoS

[10] Take down notices in USA are given under the Digital Millennium Copyright Act 1998 and Electronic Commerce Directive 2000 of the country. When such a notice is served, the host has to remove the content or disable the access to the concerned site.

attacks and so were the law firms that were working against these copyright violations and were behind take down notices (Enigmax 2010). The trend is not a feature of only United States. Portuguese organization ACAPOR which represents the interests of local movie rentals filed a complaint against Pirate Bay with the Portuguese Ministry of Culture to demand that internet providers block customer access to the site. According to the organization, Pirate Bay was responsible for about 15 million illegal downloads which had caused immense financial damage. The organization also took action against Piratatuga.net which is as popular as Pirate Bay for music and game downloads. Italy also took similar step of blocking the access to BitTorrent sites (Ernesto 2010). After one month of these actions, Anonymous retaliated by defacing the website of ACAPOR and 640 MB of e-mails data were leaked to shame the organization (Ernesto 2010). Spain's copyright society SGAE was also targeted systematically by Anonymous with DDoS attacks which crashed the site of the organization (Leyden 2010). All these attacks were part of the Operation Payback ,ost of which took place in September and October of 2010.

v. Payback Turns into Defense of Assange

The year 2010 also saw the revelations by Wikileaks under Julian Assange. By now, the events have become one of the most remembered events because the leaks were about the opaque world of big leaders and diplomats and the embarrassing truths of diplomacy and international politics. These are not the things any government wishes to tell their citizens. Political maneuvers are done very secretly often with several compromises and under the table transactions. The revelations put world's most powerful country on a back foot when its diplomatic secrets were out. The revelations could not be digested for a while and the State Department was flustered and fumbled for many days for appropriate response. The man behind the leaks Julian Assange was relentlessly pursued until he got holed up in Ecuadorian Embassy in UK after a dramatic escape all of which are part of the well known facts. He continues to stay there because of fear of arrest and deportation to USA in the event of him stepping out of the premises of the embassy. When Wikileaks happened, the companies which aided its several financial transactions including donations were pressured by US to cut off the help to the organization. PayPal was the first to be affected by such pressures because most of millions of dollars in contributions to WikiLeaks were coming through PayPal account of the organization. The account belonged to a German non-profit group called Wau Holland Foundation. PayPal permanently restricted the account of the German Foundation which was accepting donations for the website. The servers of WikiLeaks were also attacked forcing the website to use Amazon's cloud storage services which were also withdrawn. The domain name service provider of the site Every DNS was also assailed with DDoS attacks (Poulsen 2010). All these things were happening when the revelations were creating storm in the diplomatic circles of USA. The Operation Payback which was initially confined to the targeting of the copyright proponents in movie and music industry now turned to the defense of WikiLeaks. The action of PayPal and Amazon was seen as supporting the censorship of web. Therefore the two came under the hours of DDoS attacks by Anonymous which was termed as Operation Avenge Assange (Leyden 2010). Many other sites were also targeted by the hacktivists. Master Card experienced service disruption and so did Visa (Halliday 2010). An unidentified representative of Anonymous in an exclusive interview to RT's AlyonaMinkovski said: "We have been DDoS'ing sites. We have been flooding them with traffic so other people cannot use them and they cannot operate like this anymore. We have been attacking them, we have been DDoS'ing them so people can't buy things, people can't make transactions."(RT 2010). The statement in the website of the group read as follows:

> "While we don't have much of an affiliation with WikiLeaks, we fight for the same reasons. We want transparency and we counter censorship. The attempts to silence WikiLeaks are long strides closer to a world where we can not say what we think and are unable to express our opinion and ideas. We cannot let this happen. This is why our intention is to find out who is responsible for this failed attempt at censorship. This is why we intend to utilize our resources to raise awareness, attack those against and support those who are helping lead our world to freedom and democracy." (Leyden 2010).

The DDoS attacks that these groups with anarchic streaks are unleashed probably got recorded in several cyber crime statistics. Cyber crime statistics are rolled out at amazing speeds by several government organizations and private corporations because the security is the ultimate word in cyber studies in present times. But this only renders the cyber anarchists and cyberlibertarians irrelevant because criminalizing their actions takes away from them the right to have any say in the cyberspace governance discourse. Groups like Anonymous view their actions as propagating freedom in cyberspace and they convey it through their symbols of protests. The two symbols that appeared during Operation Payback and that clearly conveyed their love for values of freedom and liberty are given below. In the first symbol, the contrast in perception of the group with the mainstream understanding is conveyed. The second one is a direct attack on the copyright regime that brings several online activities under the punishable acts of piracy. In the second symbol, the noteworthy is Guy Fawkes mask. In recent times, this mask has become the most popular symbol of protest. There are two backgrounds to this symbol and its association with protests. In the contemporary period, there is a Hollywood movie which has apparently inspired people to adopt the mask as protest symbol. Year 2005 saw the release of the movie ‘V for Vendetta’. In the movie, Hugo Weaving has portrayed V, an anarchist freedom fighter who attempts a revolution against a fascist regime in a dystopian United Kingdom (www.imdb.com). The second connection with the protest comes from the Gun Powder Plot in 1605 in England. This plot was meant for revolt against King James I of England and it was hatched by a Catholic group. The aim was to install a Catholic monarch on the throne. Guy Fawkes was part of the rebels (Wikipedia.org). Therefore, one cannot miss the association of the symbol used by the present day cyber anarchists or cyber libertarians, with the anarchic elements of the past and of contemporary fiction. It also signifies rebellion against attempts by states and the powerful system of states hobnobbing with corporate. It is therefore to be expected of such actors to speak out against any signs of cyberspace governance because governance implies some kind of control and law to regulate. That means, for such actors, death of the freedom in the virtual world. But the voice of such actors has been registered more as noise coming from fringe than as contribution to the mainstream which is the power play of the states and key players in the tech and internet. Hacking and DDoS attacks are seen as signs of criminal activity by the mainstream. It is for this reason that the mainstream discourse has pushed these actors to the fringes. One of the most important evidences of this is the European Convention on Cybercrime which many in USA want their country to sign. A large part of clauses is devoted to putting in ink what the states and many corporations have been demanding: introducing legislations to criminalise certain activities in cyberspace. The portion from Article 2 to Article

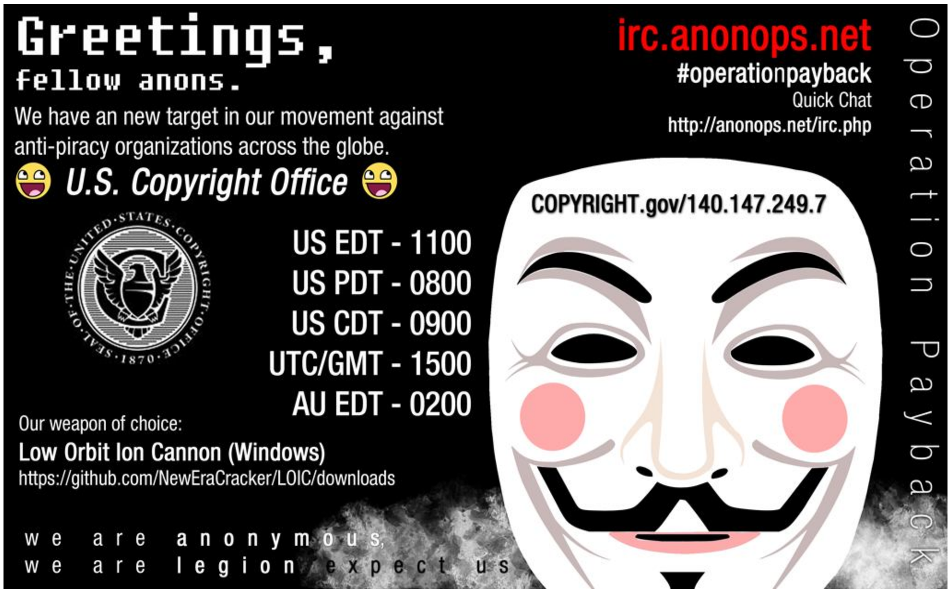
13 is exclusively about cyber crimes. Article 10 is about offences related to infringements of copyright and related rights (Council of Europe Convention on Cybercrime). The European document is so far the most comprehensive and formal piece that aims at establishing the control of state by bringing legislations. But what happens to the actors who have been hacking for freedom? They are brought under the ambit of prosecutable crimes. Below are images of protest symbols of the group Anonymous and Operation Payback.

Figure: 2.7

MENU
YOU CALL IT PIRACY.
WE CALL IT FREEDOM
ANONYMOUS NEVER FORGETS.
ANONYMOUS NEVER FORGIVES.

Source: http://en.wikipedia.org/wiki/Operation_Payback#mediaviewer/File:You_call_it_piracy.jpg

Figure: 2.8



Source:
http://en.wikipedia.org/wiki/Operation_Payback#mediaviewer/File:Anonymous-Attacks-the-United-States-Copyright-Office-3.png

2.4.2 Network Neutrality: Darwinian Principle and Equality in Access

While the copyright issue in context of cyberspace has been about how the latter is used as a resource or a platform for achieving divergent aims, the debate on network neutrality is much more ambiguous. It is as much about cyberspace as a resource as about an ideal that some want to uphold. Some have defended it fiercely while others have considered it important to the way Internet needs to function to survive in its present form. The question naturally arises as what that thing is which makes one feel strongly about it. It cannot be just about a method or a global resource. Tim Wu is recognized as the first one to discuss it from a perspective it is being done presently. In simple terms network neutrality means that ISP companies do not discriminate between services and websites. If ISPs are charging differently for differentiated quality services (providing different speeds), then network neutrality is not there because differing bands of charges will affect the speed of the services. That means that if one comes across an ISP offering a pack that says that so and so chat services will have to be done through a separate pack to avail benefits of low data charges, then the ISP is violating network neutrality (www.theopeninter.net). Tim Wu has called it an end that has to be aspired for while there is more than one way to achieve it. In order to understand Wu's case for network neutrality, it is important to know the evolutionary model of technological innovation. An evolutionary model views innovation process as Darwinian competition in which the best survives and the rest are eliminated. So the adherents of this model of innovation will not be inclined to favour a system that eliminates competition. They will not favour a process that is directed with one prospect holder because there can be unlikely biases that can prevent reaching a right decision. So if applications have to be developed, there has to be competition which will vie for the attention of the end-users. This can be ensured only by maintaining meritocracy. In language of technology, this means encouraging competition by keeping the network neutral. No application (e-mail, streaming applications like videos, etc) should be imposed on the end user. This argument is embedded in the principle design on which internet operates which is the end-to-end design. This principle basically suggests that in a network, application specific functions ought to reside in the end hosts rather than in intermediary nodes. Internet has evolved along this line and it has spread very fast. The evolutionary principle adherents look at this and argue that Internet's evolution suggests that network neutrality should not be abandoned (Wu 2003: 141-146). But this is not end of the story. The problem has begun in recent times with increasing demands from several quarters for allowing one or the other set of practices.

2.4.2.1 Significance of Net Neutrality in Present Times

Internet has not only spread fast. It has also diversified in terms of activities and services that are available on the net. Habits of people have changed with times and there are increasing demands for not just information in readable format but also videos and recordings. Therefore, streaming is becoming a popular mode of gaining information. These changes would have been very difficult had the cost of providing these services been exorbitant. It would have hampered the innovation by presenting a discouragingly high amount of operating costs to the service providers. It is doubtful that consumers on one end would have lapped up the services the way they have done now. Now, these are everywhere the net has reached. With times however, the demand for these services has risen very fast. It is from this point onwards that net neutrality assumes great significance for cyberspace governance discourse. In present times, the discourse on this is predominantly American with only US giants seen everywhere on the web with various tilts on the issue. Some justify it while others oppose it on wide ranging grounds. In the fresh memory, it is the Netflix case which has provided ammo to the debate. Netflix CEO was involved in negotiations to arrive at some agreements with the leading ISPs. The company had been delivering the content to the users by using third party transit providers like Cogent and Level 3 and some general content delivery network companies like Akamai and Limelight. Netflix now wanted to have agreements with ISPs to directly interconnect its content delivery technology with their networks as many large content providers like Google had done. But the negotiations were not successful. This prompted the CEO to urge USA's Federal Communications Commission (FCC) to redefine net neutrality because it wanted to connect directly with ISPs without any charge. It was around the time that he wrote: "A stronger form of net neutrality is required to prevent ISPs from charging a toll for interconnection to services like Netflix and other content providers." According to him, this meant sufficient access to their network without charge. The reason for this was that ISPs were "constraining" Netflix traffic to compel the company to upgrade its connections. The upgrade would affect the customers because it would involve passing off to the users whatever extra the ISPs would charge. The issue gained prominence with satirists commenting on it. A media industry analyst however damned the claims of Netflix by saying that throttling of traffic by ISPs was untrue. Whatever throttling was happening was not being done by Comcast or other big ISPs. Instead, it had been Cogent, Netflix's transit provider that had been prioritizing the retail customers over wholesale customers like Netflix. Cogent could not deny it and accepted it had done so during times of congestion. Meanwhile, the large ISPs have expressed their reluctance to go for the kind of arrangement that Netflix wants (Downes 2014). Therefore, the debate on the topic often involves the mention of Netflix.

However, the way the debate has evolved has made it look like a battle in which big ISPs are on one side and content providers on the other side. The issue is far from this kind of clear cut battle lines with ambiguities in it. Robert Mc Millan argues in Wired that the understanding on the issue has been that if net neutrality is dropped, then some content providers would have fast internet lanes while others would be expected to do with slower speeds. It is exactly this kind of argument, in his analysis, which has been questioned. This is because big companies like Google, Facebook and Netflix are already getting benefits of fast lanes. These companies have what are popularly called peering connections and content delivery systems that provide fast internet lanes. Peering happens when an internet operation connects directly to another so that traffic can be traded. This could be an ISP and an internet backbone provider[11]. A content delivery network is a network of servers set up inside an ISP that delivers content faster to home users. The big content provider companies like Google move so much traffic that they have to have special arrangements with the ISPs. This arrangement involves bypassing internet backbone and plugging directly into the ISPs. A webpage request involves many movements between browser and the web server which can cause jam. The direct plugging speeds up the transfer and the delay in accessing the page can be considerably cut down. So, content providers have opted for arrangements that allow them to directly transfer traffic from their data centers to web surfers. Therefore, big content provider companies like Google and Netflix have an edge over others. They are already getting faster lanes than many smaller players. The issue is therefore not the faster lanes. It is the size of ISPs that matters. A consolidation or presence of few big players naturally allows ISPs to bargain from a position of strength. This can lead to concentration of power in the hands of few players that can decide who gets faster access and who does not (McMillan 2014). It is also a question of muscle flexing by a big ISP company (Comcast in case of Netflix issue). Interconnection deals between big content providers and ISP companies are shrouded in secrecy creating space for anti-competitive behaviour (Reardon 2014). Therefore, those who want ISP companies not to impose charges on the content providers are demanding net neutrality.

In year 2014, the net neutrality received a mild setback when US Court of Appeals in Washington D.C. in Verizon v. FCC case ruled that FCC does not have

[11] The internet backbone provider is the one providing collection of cables and data centers that make up internet. There are many companies that provide this.

the authority to enforce net neutrality because of the way the ISPs are categorized. So the supporters of net neutrality are demanding that FCC should classify ISPs as telecommunications companies as it would give enough power to the body to regulate ISPs (Berkman 2014). This question has caused split in the internet and telecommunications industry with some supporting greater regulations by FCC while others rooting for the status quo. Big players like AT&T and Comcast feel that any kind of regulation would harm the industry but smaller players that carry traffic of Netflix have shown enthusiasm for the net neutrality enforcement. It is because they stand to lose in case the big players are able to have their way on the matter (Fitzgerald 2014). Amidst this, there have been other arguments that are related to economics, culture and morals rather than the technicalities of internet industry. The Conservatives in USA are ready with the argument that enforcing net neutrality will not be a good idea because it will kill the very innovation that has been the feature of internet (Sankin 2014). But it has its own supporters who do not reason in the same way. There are political factors that have to be factored in to understand the debate. There is freedom of speech that is a strong value for people. Tim Wu who had initially talked about the topic had opined that Internet was too important to be left to the economists and so government had a responsibility to protect freedom of speech by ensuring that certain services were not favoured for political reasons (Brustein 2014). Electronic Frontier Foundation has been known for solidly backing net neutrality for protecting freedom of expression (www.eff.org).

The above discussion is bound to indicate that net neutrality is an issue that is purely American and has perhaps nothing to do with other parts of the world involved in cyberspace. There are other instances in the recent memory that have brought to light the net neutrality aspect of the cyberspace governance. India has been in the news recently for the frenzy that use of social media has caused. Its use has spread very fast and lately has been assiduously used by leaders, prominently by the incumbent Prime Minister of the country. It is not at all uncommon for leaders of the country to comment on events and policies in the social media circuit particularly Twitter. In context of this, any issue that affects the usage of social media creates waves. Since, net neutrality is one such issue; the country is seized of the importance of the concept. The country came face to face with the issue when a telecom company introduced a pack for data services. Bharti Airtel, which is India’s largest telecom company by subscribers, introduced changes in data services pack in December 2014. The company stated that it would soon start charging users extra money for using VoIP services. In India, the VoIP services include Skype, Viber and Line. Users commonly make free calls through the internet. The planned changes included giving discounted rates only for internet browsing excluding the VoIP to the pre-paid customers (Reuters 2014). The company’s plans were panned by the media. India Today said that Airtel broke net neutrality by suggesting the changes and went “against the growing outcry for net neutrality”. The reference was actually to US President Obama’s endorsement of the principle (India Today 2014). The uproar over the issue brought to fore Obama’s comments and the American discourse on the issue. The issue which had not garnered much attention in the country all of a sudden became the central point of argument. India’s Telecom Regulatory Authority was compelled to commit to come up with a consultation paper for clarifications (Satpathy 2014). Airtel’s action in India is not a bolt from the blue. In year 2012, the company had expressed its opinion on the pricing of interconnection charges for the data services which provide internet services. The then Network Services Group Director of the company had opined that content provider companies like Google , Facebook and Yahoo! were enjoying at the expense of network providers like Airtel because network’s capital intensive nature involved heavy investment in setting up of pipes and spectrum. On the other hand, he said that they were not getting any charge on the interconnection services provided to these companies. So, he suggested, there should be a revenue sharing arrangement. The person was obviously referring to some kind of pricing mechanism whereby they could earn revenue on increasing use of data services by consumers (Thomas 2012). Therefore, Airtel and other telecom companies stand in the same position in which Comcast stands in USA. Both want revenue from the content providers. It is obvious that any kind of extra charges will discourage several uses and will hamper quite a number of innovative activities as well. If this is not enough, then there is even a more recent case. This is even a trickier one because it actually does not involve the extra charges which are the béte noire of end users. However, it can be said to facilitate weakening of net neutrality. This is the launching of Internet.org by Facebook in several countries including in India with much fan fare. The social networking giant has already launched this in Zambia, Tanzania, Kenya, Colombia and Ghana. In India, it announced its tie-up with Reliance Communications for providing services under Internet.org. According to Facebook CEO Mark Zuckerberg, India’s billion populations don’t have access to the internet and so the world is robbed of their ideas and creativity. His message came at the time of launch because Internet.org is expected to give subscribers of Reliance Communications (who have Internet enabled handsets) free access to 38 websites. The websites include a mix of entertainment, health and education related sites. Popular sites like Facebook, Wikipedia and Reliance Astrology will be accessible for free. However, the lone search option available is Microsoft’s Bing (Misra&Srinivasan,The Hindu 2015, February 11). There was initially no uproar in India in the manner it happened in case of Airtel’s data services. This could be attributed to the fact that an internet giant was talking about providing free access to some of the most popular sites. The talk of free access sounds better than talk of extra charges because the latter has the potential to pinch the pocket of end user. But eventually, it was withdrawn after it became clear that Indian Government was not in favour of weakening neutrality principle in any form.

The pros of these kinds of services are too obvious to be brushed aside. They undoubtedly promote access to Internet. But what happens to net neutrality which is like the soul of the Internet? Providing this kind of access is quite akin to providing access to all restaurants and cafes in a hotel with one time charge by the hotel. This sounds good until one realizes that there can be cheaper and more bright roadside kiosks and open restaurants that one cannot get access to with that one- time payment. Cyberspace has become what it is today thanks to all the freedom and open access which the initial wave of cyberspace brought. What Internet.org sought to provide was free access but within gated platform and only to select few sites. It meant showing the small patch of sky when one could potentially see the universe. By doing this, net neutrality is weakened because certain sites are privileged over many others. One cannot be sure whether access to Internet is possible only through this. But technological innovations have flooded the market with smart phones. Internet access is now increasingly done through handsets. Telecom companies and handset companies have introduced features that provide selective access. The cyberspace discourse has a splinternet discourse now.

2.5 Splinternet

This is related to the above discussion on net neutrality although they do not have a one-to-one relation. But lot of developments has brought a connection between technological development and movement towards a divided or splintered internet. The latter has been defined as Splinternet. There are two arguments on this. When it was mentioned by Clyde Wayne Crews in 2001, it was presented by the author as a solution to a problem. He argued at the time that Internet was vulnerable to fall into the trap of regulations by government because it was not owned by anyone and was a global commons. The governments have started regulating Internet by making myriad laws. According to Crews, it is important to escape the regulation trap. Here, he assumes a very important thing and that is that everybody does not want or need to be connected to everybody else. So, one internet is not enough in his opinion. He advocates its splintering. These splinternets will have pre-specified rules regarding privacy and will replace regulation and centralized control. He goes on to add that "what matters most is not necessarily the Internet as exists today, but Internet technology."(Crews Jr. 2011). But this is not how it is viewed now. The changes are seen with greater circumspection than the solution centric position provided by Crews. The technological changes leading to 'gated internet' with limited meaning of internet and the increasing tendency of states to control Internet are now viewed with premonition. This is because they are supposed to hit Internet where it hurts the most: the open vast space of knowledge and diversity.

What is important is why people think that Internet is splintering. When it comes to this question, it is important to look at what they assume. Here, the basic assumption is that Internet has been a vast open resource which was not brought under realm of sovereignty and proprietary rights in the initial wave of Internet age. So, that means that something has been happening that is gradually changing this aspect of the Internet. Those things are the practices and ideas that cyberspace now requires to be splitted for better goals and experiences. States want to achieve better goals like control over how the use of Internet by their population is monitored. They do not want this control to be exercised by any organization or nation. The sovereignty demands that they control of all things that can help in that kind of control. So, the instances that fit in here are the demands of countries that law enforcement agencies should have access to e-mails sent from BlackBerry smart-phones. India especially has been in the spotlight for making such demands. Similar demands have been laid at the doorstep of content providers like Google and Skype. Countries are also erecting borders in cyberspace. In digital language, it is called erecting a firewall[12] to block material deemed harmful or undesirable. China has done it and now Russia wants to erect one to rival that of China. Australia was also planning to do the same (The Economist 2010). After NSA related revelations by Edward Snowden, some countries have become even more sensitive to the need to erect just some kind of sovereign control. Brazilian President Dilma Rouseff recently echoed the thoughts of many countries at a UN General Assembly. She called other countries to disconnect from US Internet and governance structures. Her propagation of plans to create a “walled-off, national Intranets”(Meinrath 2013). It is indicative of two things. Firstly, the cyberspace discourse has now space for splinternets advocates as well. Secondly, now there are champions or leaders of this advocacy. Countries have leaders who can advocate it in the name of sovereignty and welfare of their people.

Companies on the other hand can advocate in the name of better experience. This ‘better experience’ is provided by introducing several features that slowly nibbles away open access. For instance, the new gadgets in the market are designed to be compatible with only select software. Apple has come up with such iPads that won’t support Flash software which supports online videos. This is a way to prod Apple customers to satisfy their demand for videos through Apple stores (Thompson 2010). This is a device-portal tie up which may provide better experience but eventually leads to ‘gated’ access. The Internet.org introduced by Facebook is another kind of tie up that provides access to Internet but is designed to prod people to use particular telecom company’s services. Therefore, the chain of innovations that produced many tech giants is today headed for cyberspace that

[12] A firewall is network security system that controls the incoming and outgoing network traffic. A firewall is therefore a barrier and it can be software or hardware.

has borders, gates and entry codes. Access has not become dodo yet but everything is designed to a limited view. In an analogy with universe, if cyberspace is universe then, splintering of internet will give a limited view from a small lens.

2.6 Multistakeholder Model Vs State Regulatory Model of Cyberspace Governance: False Dichotomy

It has been found in the previous few pages that actors in cyberspace discourse cannot be easily categorized as state and non-state because actors are very different from each other in terms of how they view the benefits of cyber activities to their existence or that of their values. States have differed on cyber security and non-state actors like cyber anarchists and big companies are often at loggerheads over copyrights and open access. It is for this reason that it is very difficult to have an overarching model of cyberspace governance. It has been found that whenever the question arises of having a model of global cyberspace governance, it is either the multistakeholder model or the regulatory system which gets attention. Multistakeholder model is very fuzzy. It seems to include just about everything, from the values that informed the growth of Internet to the problems of digital divide, violation of copyrights, cyber crimes and ICT for development. On the other hand, state led regulation is often understood as state control of cyberspace through institution of several cyber laws to criminalise as many cyber activities as can be imagined. In context of discourses discussed above, it is clear that there are no tight compartments. Companies want cyber laws for their copyrights while states like USA can be staunch supporter of net neutrality to save freedom of expression and innovation. So the position depends on the context in which the actors exist conditioned by the values that inform the context. Therefore the dichotomy between multistakeholder model and state regulations is not as real as it is made out to be.

The multistakeholder approach received impetus when many of the present day developments were missing from the scene. There had been no NSA surveillance bust up by Edward Snowden nor had Assange shocked the world by exposing the things that embarrass countries: dirty tricks in diplomacy. Cyber crimes had also not been noticed very widely and most importantly cyber security had not become the buzz word. Online copyrights had not gained voice nor had hackers taken with great zeal the cause of freedom to defend the essence of cyberspace. Cyberspace had just arrived in the scene in the first half of the twenty first century, young and confused when some actors came together to assert. The assertion was less about what needed to be done and more about what cyberspace ought to be. This happened in Geneva. The World Summit on Information Society (WSIS) in 2003 stated the vision and expectations from various actors involved in development of cyberspace. The key points of the Geneva principles were following:

1. People centric, inclusive and development oriented Information society where everyone can have freedom to create access, utilize and share information. (WSIS Geneva Principles: 1-2)
2. Human Rights as enshrined in Universal Declaration of Human Rights (Ibid: 1-2).
3. Challenge of harnessing ICT for development goals given in Millennium Declaration (Ibid:1).
4. Affirmation and in fact re-affirmation in freedom of expression and opinion as bedrock of the Information Society (Ibid: 1).
5. Role of several governments, civil society groups and private sector in development of ICT (Ibid:3).
6. Promotion of global culture of cyber security to strengthen confidence in use of ICT in areas of information security, network security, authentication, protection of consumers and privacy (Ibid:5).
7. Need to reduce and remove Digital Divide.
8. Need of governments to intervene in the event of a market failure to maintain fair competition and to attract investment for ICT development (ibid: 5).

The Geneva Principles were thus part of developmental perspective aimed at strengthening the principles and values that have been responsible for flourishing of Internet. Problems areas like cyber security and digital divide are subsumed under it. The Tunis Commitment (WSIS Tunis Commitment 2005) two years later only supported the aims and commitments under Geneva Principles. The Principles and commitments are meaningless without the practices. Therefore, it is important to see whether Geneva and Tunis Commitments find their reflections in the practices of countries whose support WSIS claims to have. In this regard, the policies of countries to take up e-government are interesting because they are part of efforts to meet the Millennium Development Goals. But the greatest success has been found in the cyber security. It is everywhere and governments wish to take up cyber security seriously. It has already been mentioned how cyber security discourse has gained muscle in different parts of the world. But the two statements from WSIS Summits have been somewhat sidelined with the dawn of new discourse that can at best called a race.

2.7 Cyberspace: The Most Demanded Resource

Everybody wants some cyberspace. It has become a resource, the vast space that need to be owned, controlled, utilized and appropriated for all businesses that mark the territorial world. This applies to all actors: states, corporations, MNCs and civil society groups. Also, there are no categories that can help in making sense of the discourse. On one issue, one finds states and some corporations sharing the bed while on some other issue; they are on diametrically opposite positions.

What however becomes clear is that everyone needs it. Some need it for profits while others want it to protect values. The cyber anarchists are not part of this race. They in fact are the ones who have been pushed to the fringes of governance discourse. What now remains is the race among some dominant actors. Even in the same class of actors (say, states), the participants have no consensus. This has become clearer with the two conferences in London and Budapest. The two conferences brought out in the open the differences. In the London Cyber Conference held in 2011, countries like UK, Sweden and USA staunchly defended the system that stayed free from suffocating state control. Defense of democratic ideals seemed to be the flavor among western democracies. That was a reaction to calls for greater disciplining of cyberspace. The London Conference had foreign ministers from countries speaking out in favour of the systems that they wished to see for utilizing cyberspace. The UK Prime Minister David Cameroon set the tone of the conference by stating in clear terms the expectations from the conference. He said: “The internet has profoundly changed our economies. Studies show it can create twice as many jobs as it ever destroys, and it’s estimated that for every 10 percent increase in broadband penetration, global GDP will increase by an average of 1.3 percent.” The country’s Foreign Minister said: “Nothing would be more fatal or self defeating than the heavy hand of state control on the internet, which only thrives because of the talent of individuals and of the industry within an open market for ideas and innovation.” But the foreign minister also talked about the increasing cyber attacks that are state sponsored (Ashford 2011). This was a hint at the increasing attacks that have been traced to China and Russia. Swedish Foreign Minister supported the position by saying that Internet is an important part of the wave of democracy and dignity that is sweeping the world. US Vice-President Joe Biden argued that although cyberspace was a new realm, there were older understandings to guide countries (Ashford 2011). Apart from this, the western democracies were also concerned about the intellectual property problems and the hackings that were inflicting heavy losses on businesses. Countries like China and Russia that are seen as sensitive to any kind of attempt to regime change in different parts of the world took a different view. For them, state needed to stake greater control over cyberspace (Croft 2011).

Given that this was a conference in which non state participants also participated, this looked like a platform for coming out with different needs of the countries. But whatever may have been the pronouncements of countries, from idealistic values to the dystopian need to control by state, the emphasis was on the fact that actors needed it. One year later, the Cyber Conference in Budapest saw countries speaking even more earnestly as if every word would make them win the race to grab the big pie. Western countries talked repeatedly about human rights in cyber conference. Estonian President was very excited. It was understandable because his country had taken the brunt of cyber attacks from Russia that had crippled the networks for many hours in 2007. He said: “They will want to impose their authoritarianism on us, let’s not let them do this.” It was the Chinese delegate that responded by saying: “wonder if I am in the wrong place to attend a conference on cyberspace, it seems that I could be in Geneva at human rights meeting.”(Feakin 2012). So the differences were stark but every country was possessive about it because cyberspace has been seen as a new frontier to be ‘occupied’. The occupation does not necessarily mean one that is understood in militaristic sense. This is an occupation through laws, rules and many institutions to extend a set of values. If Western democracies wish to see protected intellectual property rights and protection of freedom of expression, other countries want to crack down on cyber activities that threaten state and business. This is the reason why many countries are now planning to take control of the information sphere by not only bringing myriad cyber laws but also by putting in place system that would splinter Internet leading to what has been already discussed: Splinternet. This can be termed assertion of sovereign control over cyberspace. The militarisation and surveillance practices are the symptoms of a world gone crazy over the new resource called cyberspace. What they do is the cultivation of a new piece of space. They also provide physical existence to a sphere that was virtual only decades ago. Internet was all network and communication until it was realized that it could be zone of battle. Then came the cyber warfare and finally cyber command. Other things like cyber law and cyber terrorism were to follow very soon. Today there are as many terms with cyber prefix as there are activities in human existence. How could countries then let go of a space that they knew had done wonders for so many corporate giants and had already changed their own systems? A vast frontier that had strangely originated in small defense project labs, was lying before their eyes. So began the small steps and practices that have led one to see cyberspace being controlled and disciplined. It has been turned into a very precious resource.

2.8 Conclusion

Innovations have fuelled changes in the way wars are being waged, information shared and disseminated, resources accessed. Militarisation of cyberspace has produced systems that are transforming cyberspace into a zone of conflict. This has produced structures that reinforce ideas of cyber war, cyber offensive and cyber deterrence as On the other front, cyberspace has fallen prey to the hierarchy of power. This power emanates from domination in social, cultural, business and commercial sphere. Millions of people download movies and books, share files and use them. This sounds very easy until one finds how big Hollywood studios and production houses are crying foul over the ease with which their hard earned money and creativity takes a hit from such practices. From the perspective of many cyber anarchists and open access advocates, free access does not do any harm. In fact, they argue that such things encourage innovation. But once one crosses over to see what the government and film studios and music companies think, one finds that the argument is exactly the opposite: it is theft and hampers innovation. Therefore, any law or ruling that smacks of curbing such activities is resisted by those that wish to see completely open access. The well known hacking groups have already shown their resistance by throwing a barrage of cyber attacks on sites of organizations that are killing small platforms for sharing files and are attacking activists like Assange. They have shown that they are totally loathed to signs of governance. In their opinion, it is important to uphold freedom of expression and opinion and resist structures that kill the uniqueness that defines cyberspace. The cyber attacks inflicted by them have already been defined as cyber crimes. So, although they register their presence, they are constantly pushed to the fringes by states and big corporations. So cyberspace governance shuns them as much as they shun the former.

Therefore, the cyberspace governance discourse has been co-opted by the hierarchy that defines many other living institutions. It is already being governed albeit by many powerful actors. Whatever these actors do and say becomes source of strength for the hierarchical system that is already there. The symbols of protests presented here are the signs of resistance undoubtedly to the gradual emergence of cyberspace as a well-disciplined horse. The basis of all this have been the innovations that have produced practices among state and non-state actors.

3.1 Introduction

Cyberspace has been innovated into several applications. Most of these innovations have spread wide and have been adapted to in various degrees. The most widespread innovation is the one that has been done by cyber criminals. They have wide reach and are connected to each other through a network of computers. The types of cyber crimes range from financial crimes like cyber theft, to asking for ransom (through ransomware), snooping, hacking, defacing sites, DDoS, identity thefts, disrupting the systems through malwares, and many others that are still evolving. These activities have been the byproducts of innovating in the machine use to meet certain needs. In this innovation, the anonymous non-state actors who cannot be traced easily have emerged as key players in shaping the cyber crimes scene. Today, law enforcement agencies of many countries face the problem of tackling rising cyber crimes. Secondly, the access to copyrighted works and their free sharing without permission of the copyright holders too has been viewed a new age copyright violations. These too are gradually being seen as cyber crimes. Thirdly, the use of social media for airing grievances and frustrations has become habit of many people in a number of countries. Even countries that are known for tight government control over media have people resorting to social media. Social media was widely used in Arab Spring protests in its initial stages. Cyberspace therefore has the potential to cause political instability and that too very fast. Russia too has been through some of these developments and its domestic factors have played important role in influencing its approach towards cyberspace governance. The factors discussed in the chapter are cyber crime scene and Russia’s place in that cyber crimes scenario and the increasing use of cyberspace for generating political activism. The two are important factors in addressing the second hypothesis which attributes Russia’s cyberspace governance approach to these factors. In generating these factors, the presence of a developed Internet market has provided a flourishing environment.

3.2 Russia and the Global Cyber Crimes Scenario

Cyber crimes are one of the most talked about issues in the cyberspace governance. This is due to the economic loss that cyber crimes inflict on the targeted systems. McAfee Report in 2014 on the economic losses from cyber crimes has been very insightful with regard to the extent of losses that the global economy is incurring and the losses that can be acceptable. It arrives at following assessments:

1. In 2013 alone, the loss incurred due to cyber crimes could be around $160 billion.
2. The cost to developed countries due to cyber crimes has serious implications because they directly affect the employment creating economic activities. Citing instance of USA and Europe, the report cites that in the former the losses due to cyber crimes could cost nearly 200000 American jobs while the latter could lose 150000 jobs.
3. Cost of cyber crimes will continue to rise as more business activities move into internet.
4. The bulk of losses due to cyber crimes are incurred by the G-20 nations particularly the largest economies of US, China, Japan and Germany. These four economies alone had $200 billion. Low income countries have smaller losses but this can be attributed to the less broadband connectivity and lesser internet penetration than in developed world.
5. Internet economy generates between $2 trillion and $3 trillion out of which 15% to 20% of this value is extracted by cyber crimes.
6. Report suggests that countries will tolerate cyber malicious activities if they remain at an acceptable level which is marked by McAfee study at 2% of the national GDP.
7. Theft of intellectual property is the most serious problem caused due to cyber crimes. According to US Department of Commerce, the IP theft in cyber crimes cost US companies around $200 to $250 billion annually. OECD has estimated that counterfeiting and piracy costs companies around $638 billion annually. The Report calls it “IP theft and Innovation Cannibalism”. It is called innovation cannibalism because an innovative way of theft affects the incentive to invest in R&D to create IP. So, innovation takes a hit in the long run (McAfee 2014).

The scenario presented by the McAfee Report is not very far from the general perception about cyber crimes. Countries who are serious about increasing the broadband penetration and leveraging the internet for encouraging employment, are taking cyber crimes seriously. No corporation after all would be content to see their potential earnings getting polished off by unknown elements. The special mention of intellectual property losses due to cyber crimes has to be taken seriously in context of the several big disputes and copyright violations cases that were discussed in the preceding the chapter. This is because involvement of developed countries apart, the intellectual property losses are being borne by the big and important players in US and Europe. That makes the cyber crime an important challenge that many actors would like to tackle first. Russia here faces cyber security challenge in controlling some of the cyber crimes in its domestic arena that have fast become global. In May, 2017, when the global ransomware attacks were brought to light by several institutions hit by the WannaCry ransomware, Russia was found to have maximum infections. High concentrations of attacks suggest origin of the attacks (Wong and Solon 2017, The Guardian). The Russian President flatly denied any kind of Russian involvement, instead blaming USA for having created a malware that had backfired on itself (Titcomb and McGoogan 2017, The Telegraph). That is the nature of cyber crimes-global scale but difficult to trace. High concentration of attacks may not actually be reflective of its origin. That is why the activities of cyber criminals in one’s own territory can be double edged sword. Putin meant exactly that when he referred to backfiring of attacks. Therefore, the types of cyber criminal activities that are associated with Russia are important in understanding Russia approach to govern cyberspace. The first in this is the presence of hackers in Russia.

3.2.1 Cyber Crime Ecosystem in Russia

Russia appears to have some spots that are sources of cyber crimes. According to an investigative study titled *From Russia with Code: the Next Generation of Cyber Crime*, Russia is ground zero for cyber crimes. This study has been done with the help of inputs given by unknown Russian hackers who can easily pull million dollars of cyber heists very smoothly. Explaining the modus operandi, the author of the short piece explains how an ace hacker called Kislitsin shows the author the whole thing. He chooses an IP address of Chicago, logs on to hidden forums to pick up a cyber tool to infiltrate like Trojan or some program to infect computers which is used to infect unsuspecting computers. The unsuspecting computer then becomes infected and a part of vast network of botnet[13]. It is such unsuspecting computers that are then used to pull of theft of balances, passwords and other details. Once a computer has been compromised, the next step is to transfer money. The Russian hackers call it *autozaliv* in Russian language. An autozaliv involves role of another infecting program that can be obtained with as much as ease as the earlier Trojan. So when the unsuspecting person logs on to banking profile, the hacker directs the infected but unsuspecting computer to transfer the amount into another account automatically. It is even possible to obtain the control of infected computer's banking screen so that the bank account of the targeted person would show the amount that he/she wants to see while in reality the money has long changed its place. The money then goes through channels of what are called in the hacker circle as money mules that provide illicit courier services to make transfers. The money changes hands from one money mule to another until it reaches the cyber criminal who has pulled off the heist! (Topol 2014). In 2012, Max Goncharov had shown in a detailed study on the market of the cyber criminal underground in Russia. His study is indicative of the extent to which the cyber criminal activities have put on sale all the things required to conduct cyber heist. These things are being sold at a reasonable price making the whole underground a grey market. As a sample, basic statistical crypter is available at $10-$30, dedicated servers are available at $0.50-$1 and powerful servers at $10-$20, one day DDoS services at $30-$70, cheap e-mail spamming services available at $10 per 1000000 mails and so on. In other words, the Russian hackers have not the things available only few clicks away but are also fuelling the underground cyber economy by marketing these things among prospective buyers. This is attested by several advertisements which circulate in internet and are not even noticed by unsuspecting people. The same advertisements however are of great interest to the hackers who want to hack to make some extra buck (Goncharov 2012).

[13] Botnet is a network of infected computers that take command from the perpetrator or controller to spread the malware in more computers

The new data suggests that prices of many of these programs and services have fallen sharply indicating that either the availability has increased or the cost of obtaining them have gone down considerably. These indicate that it is now even cheaper to conduct the cyber criminal operations that are aimed at stealing. But despite the falling prices of services, the underground activities are still profitable. The facts suggest that prices have fallen, among other reasons, due to automation. So, the cyber underground members are as tech loving people as any other corporation is. Russian underground sellers are also promoting use of Deep Web[14] which provides optimal environment to sell illegal services and programs with anonymity. According to one analysis, the Russian cyber underground economy started as a peer-to-peer sharing of malwares and services but the same has gradually attracted now even higher skilled computer experts (Paganini 2014). It looks like the automation has attracted the more tech savvy people into the grey zone. Russian Business Network which actually sounds like the name of company is in reality a network that provides a whole kit and infrastructure to do malicious activities in cyberspace. It is better known by its shorthand name 'RBN' and is the most popular name in the underworld of cyber crimes in Russia. With such a name having gained notoriety (Bizeul 2007), and flourishing and well organized underground activities, Russia can be easily expected to have quite an important place in cyber crime discourse. That is indeed the case. Russia has been even tagged as the cyber crime capital although Joshua Keating while mentioning the arrest of a Russian hacker in Guam by US and filing of charges against another Russian doubts the basis of the tag. He cites China and Indonesia, the two countries who are way ahead of Russia as source of cyber attacks in this regard (Keating 2014). United States which has borne the brunt of hacking originating and benefiting Russian hackers, has taken the problem seriously. Recently, USA's FBI declared Russian national Evgeniy Bogachev 'wanted' and have put a reward of $3m for information leading to his arrest or conviction. Bogachev is allegedly involved in several cyber criminal cases (The Guardian 2015).

[14] The Internet that people commonly see and use, is just tip of the iceberg. Deep Web is the part of the Web that is totally unregulated and even unknown world of web in which one can operate anonymously. Anonymity ensures that much of the Deep Web activities cannot be traced. Deep Web cannot be accessed through normal browsers and require special browsers. These are used by people from various walks of life: criminals, drug dealers, assassins, intelligence people, investigative journalists, and so on.

Bogachev is known to be a resident of a place called Anapa which is a beach resort in Black Sea coast. According to the Telegraph, despite the FBI’s actions, the Russian government has not pushed the matter much and is not betraying any inclination to extradite him. This thing apart, some locals hail him as hero and are happy to see that he has served the Americans right by causing them losses. He and his hackers have already made away with $7 million from bank accounts across USA with the help of a malware now popularly called GameOverZeus (GOZ). Zeus in Greek mythology is considered the Father of Gods and men. He is believed to have fathered many gods and mortal and semi-divine beings. This means that his genes are widespread. GameOver Zeus is also a widespread botnet similar to the progenies of Zeus. Bogachev only seems to have benefitted from this widespread network. The bigger question however is why Russia is having a conducive environment for the cyber crimes underground. David Bizeul finds that this may have a lot to do with the hacking culture in Russia. Russia has been known to have talented virus writers and the philosophy of hacking comes naturally. It is an attitude that is present in tech savvy young people in the country. But IT sector has not been able to generate enough employment in the sector for such minds resulting in these people drifting to the underground sector to earn extra bucks (Bizuel 2007). It has been found that highly skilled engineers and mathematicians are offered $24000 a year, an amount which is not enough to lead a satisfying life in Moscow. So, the attraction of the cyber crime is real where the money is good. Moreover, Russia does not seem to take this seriously until the hackers target the country’s economy and institutions (Plesser 2014). The attitude therefore seems to be that as long as the hackers are robbing the riches of other countries, there is no need to give oneself headache.

Something similar was there when Soviet Union broke up. But that was then and that too happened in a nuclear context. Russia was seen by the western countries as a red zone where nuclear smuggling was becoming rampant and the unemployment was forcing talented scientists and technicians to sell off strategic secrets and fissile material. Some of the stories indeed were true but many of them looked like nightmares expressed by the American strategists. Russian nuclear weapons remained safe and no terrorist organization ever got the fissile stuff from any Russian source. The perceptions about Russia in matters related to cyber crimes like hacking are not very far from the kind of hysteria induced by nuclear strategists earlier. The only difference is that the one about cyber crimes does not push one to press the emergency button. Russia still comes across as part of the problem in perception of West which may be a little misplaced because according to a study done by Symantec (the US headquarted American Software Company), Russia is below at 12th place in the ranking of 20 countries. The ranking of countries is based on degree to which they face or cause cyber crimes. In compiling the list, six factors were taken into consideration. Malicious computer activity, malicious code rank, spam zombies rank, phishing web site hosts rank, bot rank and attack origin. (Enigma Software, URL: https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/).

There are two ways in which this perception affects Russian role in international cyberspace governance. Firstly, since cyber crimes have attracted the adverse attention, this is bound to affect the way any future bargaining takes place among state and non state actors. Corporations and banks that have lost millions to the cyber crime black holes in Russia will not be keen to listen to the country while it is promoting a bigger role of state in cyberspace governance. Having a tag of cyber crimes centre makes one a part of problem which can be turned into solution only after lot of efforts to bring about an image makeover. Secondly, cyberspace crimes are such that they do not have many separating doors and borders. The same people who are pulling off several cyber heists can someday turn their guns inwards. Having cyber criminals in one’s own backyard poses cyber security threat. It only means extra homework for the cyber sleuths in the country and more laws. Worse are the losses that they have potential to inflict.

3.2.2 Online Intellectual Property Theft in Russia

Russia once again occupies an uncomfortable position on account of intellectual property theft. Music and games are one of the most popular things that are downloaded and shared. It has been the claim of the creators and copyright holders of these that such downloads in social networking sites are illegal and lead to losses. There are basically two names that have cropped up in the copyright violations in online space. These two have generated lot of friction due to involvement of interests of well known American companies from entertainment industry. Since the companies have been American, the issues have been irritants in Russia's trade relation with United States as well. There have been few well talked about cases that have brought into limelight the copyright violations in online space in Russia. The first case pertains to the site AllofMp3.com. This company or site has been sore in the eyes of copyright holders particularly the ones from music and film industry. It is due to the model of operations that the company has developed. Firstly, it became extremely popular and well perched in the minds of Russians because the music service provided by the site (until around seven years back) contained no Digital Rights Management. These gave scope to the consumers to copy and transfer the purchased song or music to device on his or her choice. The roster of file formats in which most song tracks are available is also quite diverse making consumers happy. Even the price of tracks available on site was such that they could make even file sharing sites like Napster sweat. This site became quite a problem when the recording labels called it illegal. International Federation of Phonographic Industry (IFPI) called it illegal. (Mennecke 2006). In June 2006, it was reported that file downloading site could jeopardize bigger trade interests of Russia. Russia was negotiating with several countries for a much coveted entry in World Trade Organization. The trade body is rather notorious for its staunch backing to a strong IP regime and it is not uncommon to see member countries slugging it out over some copyright or patent thing. IP issues are therefore almost sacred to WTO and even more to US whose interests are bigger. So, when the issue of AllofMp3.com started creating noise, the American trade negotiators warned their Russian counterparts that Russia's entry could face roadblocks owning to lax IP regime and particularly the concerned site. This happened after the recording labels like Warner, Universal and EMI failed in their efforts to budge Russian prosecutors. The Recording Industry Association of America was exasperated in 2006. Its executive vice president Neil Turkewitz said: "It is totally unprecedented to have a pirate site operating so openly for so long." AllofMp3.com responded to the charge of "being illegal" by citing a license issued by a collecting society called Russian Multimedia and Internet Society. Russian 1993 copyright law permitted collecting societies to act on behalf of right holders who have not authorized them to do so. Due to this provision in the old law, the collecting societies were gathering royalties for foreign copyright holders without their authorization. But more than the technicality in any law Russian or any other, it is the popularity of the site that has been the cause for heartburn among the recording companies. Russian company was attracting consumers from Britain and United States, the countries which consume English music. The number of users in USA was increasing at a fast pace according to Comscore (Crampton 2006). AllofMp3.com responded with a detailed statement in which it made following things. In a detailed press release titled ‘Setting the Record Straight’, it said that it was important to come with a statement because the US government officials and politicians had been demanding the shut- down of the site and threatening to impose sanctions and to block the entry to WTO. It made the following clarifications (Reid 2006):

1. AllOfMp3.com belonged to a Russian company and it was fully in compliance with the Russian laws and Russia had till then not detected any breach of law by the site.
2. The site was not operating or advertising its business on the territory of other countries.
3. The site had regularly transferred “substantialamounts” as royalty payments to Russian organizations for “collective management of rights.
4. The site reserved the right to take steps to protect its business reputation.
5. The site had been making direct agreements with right holdersand authors and were increasing the price of the music compositions and transferring the royalties directly to the artists and record companies.

The fourth statement which talked about protecting the business reputation because IFPI had called it ‘illegal’ and a recording association of USA had called it a ‘pirate site’. Pirate is a strong term because it amounts to calling the organization a thief. It also means that the site had no originality to offer. In the world of business, stealing someone’s original work hinders the growth of goodwill and tarnishes the reliability. Users and customers cannot imagine taking services from a company which is being accused of breach of law. One would not be inclined to rely on a site that may shut its shop tomorrow. Therefore, the site asserted strongly its right to respond to allegations that according to it were baseless and based on incomplete information. But despite this clarification, recording labels filed a law suit in New York against the company. The plaintiffs included Arista, Warner Brothers, Capitol, Universal and several other companies.

The lawsuit stated that the defendant's (i.e. Mediaservices, the company handling the site) entire business amounted nothing more than the infringement of exclusive rights granted under Copyright Act and New York law, to the plaintiffs (Out-Law.Com 2006). The company responded to the $1.64 trillion law suit by dismissing it saying that "AllOfMp3.com does not operate in New York" (Arrington 2006). The music labels pressed Russia for prosecution which was done. The company owning the site was however acquitted of the copyright infringements charges in 2007 (Reuters 2007).

In the Russian market for download and sharing of music, there is another very popular platform which is the social media. It is Vkontakte in Russia. The term means 'In Touch or Contact'. Widely regarded as the Facebook of Russia, it was founded by Pavel Durov, a young man of thirty years who is as charismatic as Facebook's Mark Zuckerburg. The copyright problem began to raise dust in 2013 when once again the music and film industries began to express exasperation with the way social media platforms in Russia were encouraging people to do things that infringed upon the copyrights. In 2013, Vkontakte had faced the heat from some music labels for unlawful distribution of around 6000 tracks of famous singers like Madonna, Linkin Park, Metallic and Beyonce. At that time, the founder of the social media company was balanced and almost conciliatory in his response saying that "If some music companies wish their content to be deleted from VK, we, as always, are willing to comply with their wish. On the other hand we are also ready to seek mutually beneficial ways to monetize their content. This year we managed to find such solution for video content and we are optimistic about the audio section of the VK as well"(Lunden 2013). Then, In February 2014 as expected, United States expressed deep concern about the Russian social media company Vkontakte's role in copyright infringements. US Trade Representative included the name of the company in the Out of Cycle Review of Notorious Markets as a pirate site that encouraged counterfeiting. The company had already been included in the list four times before this (Amroon 2014). The Out of Cycle Reviews by USTR Office List is made under the Section 301 of the US Trade Act of 1974. This statute is for identifying the trade barriers due to inadequate protection of intellectual property. Such countries are identified by April 30 of each year and are submitted in the Special 301 Report of USTR. There are several countries in the list. Even some countries following the rules under the Trade Related Intellectual Property Rights (TRIPS) of WTO are in the list because they do not follow the stringent requirements of (United States Trade Representative) USTR Office or their law. Therefore, having the name is not a shocking thing that can push a social media company that has the gumption to coolly carry on the work. When countries are not being spared, what change can one company bring to change a pattern? After all, it is not a forgotten fact that several other sites across the globe are earning money by doing the same thing. In this context, copyright battles explained in the preceding chapter are indicative of the trend that has picked up in the cyberspace as resource for business. Vkontakte is aware of such things. It is probably for this reason that they did not give a knee jerk reaction to the USTR actions.

Later in the year, it was reported that the top music labels proceeded against the company by filing three separate lawsuits in St.Petersburg and Leningradsky alleging this time that the company was complicit in violating the Russian copyright laws. The three companies were Sony Music Russia, Universal Music Russia and Warners Music UK. The site initially did not respond to the lawsuit action. Its site only stated that it had no right to undertake the roles of law enforcement and judicial authorities and was not in a position to objectively evaluate whether the content was illegal. It further explained that the applicant who felt the content was illegal should seek help from law enforcement authorities and the court of law. The statement advised the copyright holders to contact individuals first before filing complaint with the site's administration (Essers 2014). Recording Industry Association of America (RIAA) found the actions of sites like Russian Vkontakte and Chinese Sogou "offensive" attributing the actions of these to the bad intentions to launch music without services without any form of licensing as "a cynical ploy to gain market share and make money"(www.riaa.com, 2014). Too much involvement of American and other western companies may give one a feel that these issues are some sort of bilateral problems. It can be said these problems have that dimensional as well because American policy has been fussy enough in trade matters where they do not seem to get a good bargain. However, despite the shadow of the bilateral aspect, this is not about Russia facing the rest of the world. Russian music recording industry has been equally worried about the illegal download. In fact, Russian film producers and anti-piracy activists were active in welcoming a new copyright law introduced by Russia that had supposedly improved over earlier one in 2013. Konstantin Zemchenko, who heads the Russian Anti-Piracy Organisation (RAPO) and has the support of Motion Picture Association of America welcomed the move by stating: “We wanted more and had proposed that the sites themselves should legally have to filter out pirated content but this was fought by powerful providers such as Google. Russian film makers like Sergey Selyanov which has the reputation of producing Russia’s box office successes was pleased and said that piracy was a huge problem that had increased due to increased broadband penetration (Holdsworth 2013). The support of a major American body that has already created troubles for many file sharing sites indicates that the support to the goal of copyrights cuts across the borders and is not a bilateral problem. It is the however the USTR actions that give it a flavor of bilateral dispute. In this context, it has to be argued that when cyberspace has emerged as a space or resource for business that can fetch real profits, the old set up that defined what all could be shared is bound to come under stress. The emergence of file sharing sites and the strong resistance to them as in Russia and other countries are signs of tussle that have the potential to bring a turning in the way countries would cyberspace. Governance means having some laws to control the particular sphere. Copyright laws and their defense or violations fall into this groove. Since most of the entertainment material is available in cyberspace, these are posing unforeseen situations that are bleeding the old model of innovation.

3.3 Russian Internet Industry

An Internet industry includes a whole universe of businesses and services that are based on internet. In very basic understanding, some companies in the internet industry are doing the things that people have been doing since ages but in ways that are entirely new. That keeps the internet industry apart from other industries. Since, it has been argued that innovations and spurt of new models of businesses are the reasons for so many copyright violations, it is important to look at innovation in Russia. On the face of it, Russia does not come across as the country that has led the world in innovating the Internet, but the reality is far from it. In a world dominated by the American Internet giants, that kind of notion takes root.

Russia however has picked up the pace and the internet industry looks interesting now with the emergence of some very key players with the financial muscle to make acquisitions. In 2012, the Moscow Times reported its list of top twelve web companies that were providing a diverse set of services. Most of them belonged to the e-commerce category that provided some services or were some sort of entertainment providing platforms. The Moscow Times found the reason for their success in the localization of services and application of some experience that had to do with their Western background. The types of services were indeed an interesting long list. Oktogo.ru which offered the largest selection of hotels in Russia had won the 2012 National Georgraphic Traveler Awards 2012 in the best internet service category. Jelastic, funded by Almaz Capital and Runa Capital has been attracting web hosting customers. Onetwotrip has been doing superb business in selling the airline tickets online. Dvenik.ru has been providing a unique online school service in which more than forty percent of the secondary schools have signed up. Hopesandfears.com founded by former journalists from the Russian edition of Forbes magazine, provides online journal. Its Look At Me, its magazine, has become one of the top Web magazines in Russia. Grishin Robotics founded by CEO of Mail.ru focuses on investing in technologies in personal robotics (Sadchikov 2012). These are the names that the Russian newspaper has listed in the top ten internet companies. These however are smaller players and do not include the ‘big players’. The big players are actually those whose names come first whenever any web search is done on the internet in Russia. These are just few names and need to be discussed in a more elaborate manner. They are Yandex, Mail.ru and Vkontakte. In present times, they just cannot be ignored owning to the status of almost the Russian internet giants and their widespread use in the country.

Yandex is one of the most powerful search engines of the world. It dominates the Russian market by doing the same things that Google is doing that is advertising, offering free mail hosting service, data rich mapping service and several apps to improve productivity. It is so much in the minds of Russians that the term Yandex is used both as noun and verb. According to the company’s international media relations, Russians describe Google by calling it ‘the Yandex of USA’. It is already dominating in the neighbouring East European countries but it is making attempts to expand to Turkey by migrating its services and products to the non-Russian world where the script is not Cyrrilic. Yandex has registered its presence in Turkey and now around forty percent of Turks are familiar with Yandex. It has tried to touch the hearts of the locals by adapting its app services to the native culture. In this regard, it has introduced a Ramadan App which alerts people when the sun rises and sets (Dillow 2013). According to the first quarter result, the share of the Russian search market has been almost 62 percent with search growing at 21 percent from the first quarter of last year. According to CEO of the company, ArkadyVolozh, the search engine enjoyed growth in the number of advertisers. The growth in advertising was reflected in the ad revenues that went up by 39 percent since the first quarter of 2013 (Gesenhues 2014, Fortune). Yandex however faced competition from Google and the two got locked in some sort of competitive tussle not very long back. Google opened its Russia office in 2005 at a time when the company was spreading its wings wide and Russia was enjoying a good time thanks to the fat oil and gas revenues. The market conditions were looking up in that year and country's ruinous decade of 1990s had become past. So, there was a confident company that entered an equally confident country.

But Yandex and Google serve the same things. So, the competition was inevitable. Their similarities hold key to the competition between the two in Russia. Both search engines have been earning revenues from text based advertisements. Secondly, the two have shown enthusiasm in diversifying their business and have ensured that they get revenues from the display ads and are able to do business in the online retail comparison shopping service. There was a market perception few years back that Google would nibble away Yandex's share gradually. Given the similarities that have been explained, such a perception was not entirely misplaced. However, things turned out to be a little different. This is due to the few differences that keep them apart. Yandex is more diverse in terms of services that it offers. So according to an assessment of the nature of Yandex, the Russian search engine is actually more than just a search engine (Investor Business Daily 2013). That however does not mean that the two never faced problems from one another in Russian market. In 2015, Yandex filed a complaint with the local anti-trust authorities against Google for the latter's practice of keeping its rivals' services off the Android[15] powered phones. Yandex's complaint was that Google was bundling Android phones with the Google search engine. According to the company, the device manufacturers should have a search engine of their choice. Google according to the Russian company was preventing manufacturers from pre-installing competitor apps. In the opinion of some industry analysts, Google had managed to gain some inroads into the Russian market thanks to the increasing use of smartphones and other mobile devices that had Android operating system. In fact, it has been found that around 86 percent of the smartphones sold in Russia had Android operating system. Some Russian cellular equipment manufacturers have notified the Russian company that it was no longer possible to pre-install Yandex services on their Android phones (Zaks 2015). In the context of complaint filed by Yandex, it is important to look at things from two perspectives. From a market competition perspective, it is a good way to prevent a rival from establishing in the market through unfair means that block competition. The other side is that Google's action has other reason to attract attention. It is that it is not only the Yandex that has felt uncomfortable with Google's practice of bundling[16] its services with the Android operating system that is the dominant operating system in mobile phones.

In Europe too, Google attracted adverse attention. Microsoft, Oracle, Nokia, Expedia and some other companies formed a group of 17 high tech companies filed a complaint with the European Commission over the Google's offerings in Android powered phones. The complaint was aimed at asking the Commission to protect competition and innovation which as per the demand implied that Google's bundling practice was killing competition and innovation (AFP 2013). Since the objective of the complaints and the action demanded of the authorities

[15] It is a mobile operating system currently developed by Google and is designed primarily for touchscreen mobile devices such as smart phones, tablet computers. It uses touch inputs that loosely correspond to real world actions, like swiping, tapping, pinching and reverse pinching to manipulate on-screen objects, and a virtual key board. A mobile operating system as opposed to a normal operating system used in desktops and laptops, has features that are useful for mobile and handheld devices. The essential mobile features are: a touchscreen, cellular, Bluetooth, Wi-Fi, GPS mobile navigation, camera, video camera, speech recognition, voice recorder, music player and near field communication.

[16] According to Investopedia, bundling is defined as a marketing strategy that combines products or services with the purpose of selling them together as a combined unit. It enables purchase of several products or services from the same company. These products can be related or dissimilar but one that cater to one category of customers. So, for instance, two different kinds of insurance can be purchased from one company that is offering the bundle of two, instead of buying them separately from two different companies.

were similar in the Yandex and Europe, it can be said that anti-trust complaint was not made out of sheer fear of facing a rival. It is also important to look at the splintering tendency that Google's practice has. The bundling practice has the impact of inducing people with Android systems to use Google services. That restricts the information that can be accessed and by virtue of that results in splintering the net as discussed in second chapter.

Splintering as an effect of the practice of bundling therefore can have implications for the market. It does have the potential to create conditions that lead to a domination of one player in the information. But it is conditioned on the manufacturing of devices that allow for bundling. Nevertheless, bundling as noted in the Yandex complaint and earlier in the European Commission means that governments will have a homework cut out for them. Anti-trust and practices encouraging monopoly conditions are always in the radar of governments throughout the world. Governments therefore are dragged into something that affects what one gets in the screen of smart-phone. This particular thing of bundling means lot for cyberspace because what one looks for and what one finds in an information sphere depends on how much choice cyberspace provides to people in countries. Russian anti-trust authorities were therefore not faced with the normal complaint that could be resolved by passing a rule that debarred a certain practice. The bottom line however is that Yandex was not facing an urgency that required it to restrict Google because the market share of former was high enough to give it a cushion at least in short run. But the smart-phones are everywhere and that could not be ignored. One would be tempted to say that information has the potential to make a small device strong relative to the Goliath of any company that is slow in catching up with its pace.

Yandex is not all that Russia has got. There is another player which has become quite a rage similar to Facebook and Twitter and that is Vkontakte. Apparently, Vkontakte does what Facebook does, that is, provide social media and enables people to connect with one another. There are lots of similarities. But what sets apart Vkontakte is the spirit which was infused by its young founder CEO, Pavel Durov. Pavel Durov left Vkontakte quite some time back to start new venture but he still symbolizes Vkontakte, giving it the libertarian perspective by holding on to the practices that allowed freedom of expression in the face of goliath Russian state machinery. It is not easy to do business if the venture has allowed people to vent out their anti-government feelings. But Vkontakte did exactly that and Durov held his own, using creativity to unleash what is not possible through other media outlets. Launched in 2006 along with a friend much like Facebook, it went on to establish its presence across Russia and particularly in their minds (Johnston 2015). It symbolizes Russian social media even though Russians use other platforms as well. In this context, it is important to discuss how the presence of Vkontakte and Facebook have changed the way people participate in politics when they are not voting. One of the forms of participation is expression of dissent. Social media outlets like Vkontakte and Facebook have facilitated new forms of protests that allow for expression of disgust, disillusionment and mockery. It is quite interesting that thanks to the two social media outlets and entry of Twitter later has created a strong blogging culture in which political claims and counter claims are made.

3.4 Political Activism in Online Space

Political activism has taken roots in online space in Russia very fast. It is visible in several forms and practices and there are now numerous instances of it. Alexei Navalny is a famous political activist and Russian blogger. Through his blog, he has made several claims that have affected the credibility of Russian Federal Government. The claims have been related to the corrupt practices. He has been associated with several exposes but some have been indeed akin to earthquakes putting the government and their corporate cahoots in a tight spot. In the East Siberia Pacific pipeline matter[17], the blogger obtained documents that showed that full audit report of the East Siberia-Pacific had revelations related to big theft. The audit was done in 2007 and was published only in part. The indicting part was not released. Navalny published the remaining part which had information indicating theft. This is the pipeline that is being done to supply crude oil from Siberia to the

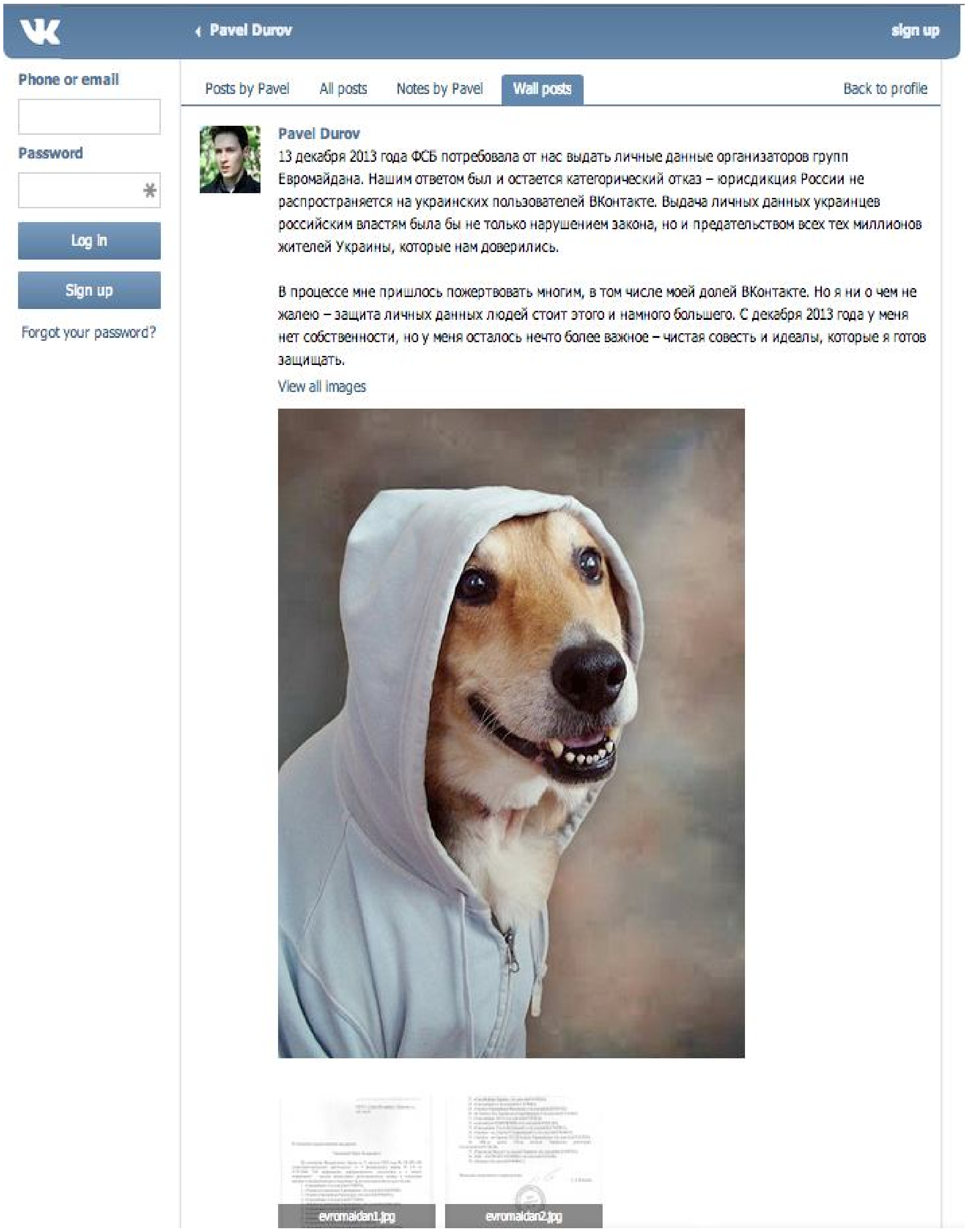
[17] Transneft was the company that got the contract for constructing the pipeline (called East Siberian pipeline) to the border of Russia with China. Alexei Navalny's report on the project found that Transneft inflated the estimated project exploration costs and stole more than ten billion rubles. Navalny who is anti-corruption activist and blogger, sent official letters regarding this matter to various law enforcement agencies, asking them to open embezzlement investigations. But, according to him, no action was taken. In addition to this, he alleged that documents related to this were destroyed. In 2010, an official leak also showed that around $ 4 billion was stolen by the Transneft in the building of the pipeline.

Pacific Coast to the Asia-Pacific markets. The details of the revelation that were posted in the blog quickly spread like wild fire and attracted thousands of comments in 2010. The response of the Transneftcompany was that “it does not respond to the personal records of third parties”. The company spokesman dismissed the whole thing by arguing that a blog was akin to writing graffiti on a wall. He was quoted as saying: “We are not talking about publishing but a recording in a personal diary. I will not comment on any entry in personal diaries.” (BBC News 2010). But a year later, he exposed the malpractices in Russian Parliamentary elections by posting videos of the wrong methods to win elections. Navalny was arrested and was charged with several corruption cases. But the videos did the job. Thanks to Vkontakte and Facebook, they got circulated among the users of the social networking sites. Twitter joined in with the wife of arrested blogger taking up the twitter feed of the blogger and the videos of the protests were spread and streamed live. Many people pledged to join the protests against the government. The clips were quite stunning given the claims of popularity of Putin that his supporters had been making in media. When election results showed that United Russia, Putin’s Party was leading, many were disgusted and shocked. But the videos revealed how that had happened. One clip for instance gave a bird’s eye view of an election official ticking off a stack of ballots and preparing them to stuff with votes for United Russia. Other videos had evidence of repeat voting. According to Konstantin von Eggert, a commentator for *Kommersant* FM radio said that “whole thing works like a snowball”(Carbonnel 2011). The reference was obviously to the way it started with a blog and gained groundswell support in the form of anger towards the establishment in Kremlin. Even though Putin was Prime Minister at the time, his powerful personality and his shadow were difficult to get overlooked by people. So the online outburst became a protest against became directed at Putin. Both Vkontakte and Facebook gave links to the protests. Bloggers and activists gave call for people to gather at different points to protests on these sites. The anger was fuelled by the links provided by the social media sites which had the videos of the elections.

According to another Russian blogger AleksandrMorozov, the videos played an important role in organizing and persuading people to come to the streets. In his opinion, without these social networks (Blogs, Vkontakte, Facebook and Twitter), people would not have had been able to see the extent of corruption and elections violations (Balmforth 2011). It is not that Russian government officials and office bearers stayed away from social networking sites. Rebuttals of acrimonious nature were made by allegedly none other than the highest office bearer Dmitry Medvedev who was President at that time. Known as tech savvy, his retweet created frenzy firstly by the nature of the retweet and secondly by the fact that he was President at the time. Alexei Navalny had earlier called Putin “a cocksucking sheep” and United Russia Party “a party of crooks and thieves”. In response to the Navalny’s description of the party and its leader, a media savvy Duma deputy wrote a tweet: “Today it became clear that a person who writes in their blog the words ‘party of crooks and thieves’ is a stupid, c*cksucking sheep☺”. In a late night tweet, President Medvedev retweeted the tweet. Kremlin denied that Russian President had done so. It further said in a tweet that it was incorrect and had happened due to some “inadmissible intereference in @MedvedevRussia’s feed” (Elder 2011, The Guardian).

The other thing that raked up dust for a while was a series of Euromaidan protests. These protests began around November of 2013 with a groundswell of sentiments against Ukrainian President Victor Yanykovych. Some of the Euromaidan protesters coordinated and organized on social media platforms. Since Russia’s Vkontakte got embroiled in the Euromaidan protests, it is important to discuss how these protests began. Euromaidan as a term has become now synonymous with all that triggered the present Ukrainian problem. But it actually began when Ukraine was going to sign a trade agreement with European Union. This signing meant that Ukraine was formalizing its joining of the western camp. Russia did not take this very kindly and made a chastising measure by stopping all goods coming from Ukraine. It amounted to arm twisting through trade channels. For some time, the measure worked because Ukraine stopped negotiations with Europe over the agreement that it was going to sign. In November of 2013 when an EU summit was held, President Yanukovych attended it and both sides made it clear that agreement would be signed at a later date. Before that, a chill had fallen over the relationship when Ukraine told EU that agreement would be signed only if dip in trade and relationship with CIS are compensated for. Around this time only, a twitter feed was formed called Euromaidan combining the term ‘Europe’ and ‘Maidan’, the latter meant a square or open space of the Freedom square in Kiev. Later this feed was used to propagate the anti-Yanukovych sentiments and to organize the ground protests in the country. Yanukovych has been seen as leaning towards Russia. In fact, when protests broke out and were going to threaten his life in February 2014, he had to flee. He escaped to Russia with Russian help and gave the statement later that he was the legitimately elected President (Frizell 2014; Radio Free Europe 2014). Vkontakte is popular social media platform in Ukraine and East European countries. The social media campaign that began in Twitter spread to Vkontakte and many of the organizers of Euromaidan were present in Vkontakte as well. It was the revelations related to this and made by Pavel Durov that gave insight into the paranoia that social media had created in the mind of Russian Federal government. He posted on his Vkontakte page the whole thing, telling how Russia’s FSB, the successor agency to KGB had pressured VK over Euromaidan protests. He wrote on his VK page that: “On December 13, 2013, the FSB demanded from us to turn over the personal data of organizers of Euromaidan protesters. Our response has been and remains a categorical refusal-Russian jurisdiction does not extend to Ukrainian users Vkontakte. Giving personal details Ukrainians Russian authorities would not only be against the law but also a betrayal of all those millions of people in Ukraine who have trusted us.” He further explained how in the whole process he had to sacrifice a lot but had nothing to regret over because protection of personal data of people was worth that (Ries 2014).

Figure 3.1



Pavel Durov

13 декабря 2013 года ФСБ потребовала от нас выдать личные данные организаторов групп Евромайдана. Нашим ответом был и остается категорический отказ – юрисдикция России не распространяется на украинских пользователей ВКонтакте. Выдача личных данных украинцев российским властям была бы не только нарушением закона, но и предательством всех тех миллионов жителей Украины, которые нам доверились.

В процессе мне пришлось пожертвовать многим, в том числе моей долей ВКонтакте. Но я ни о чем не жалею – защита личных данных людей стоит этого и намного большего. С декабря 2013 года у меня нет собственности, но у меня осталось нечто более важное – чистая совесть и идеалы, которые я готов защищать.

Source: http://mashable.com/2014/04/16/vkontakte-founder-fsb-euromaidan/

Above is the page of the post in which he explained the whole thing, with a picture of a dog with a hoodie. It was a humorous way to express dissent. Below the photo are the two documents that show that FSB indeed had ordered Durov to hand over the details. Earlier too, he had come under pressure of FSB for turning over the personal data of the users who were anti-corruption protests. In fact, Durov is no more living in Russia and has left Vkontakte. Nevertheless his leadership of Vkontakte and his influence over the social media and blogging world because of his candidness and forthright attitude towards expression of political dissent has ensured a healthy civil libertarian culture in Russia and in the neighbouring countries where Vkontakte is used extensively. The Euromaidan protests and the fears of FSB in fact are a reflection of how much power Russian social media venture has achieved in terms of influence.

Russia has also witnessed emergence of novel methods of online protests by relatively small players in the country. For instance, Pirate Party is a name that has emerged in the scene lately due to its completely unambiguous stand on the copyrights. It provides web hosting[18] services to a number of sites and its ideology is libertarian with total opposition to the copyright regime. Its website piratehost.net describes the ideology of the body by talking about the legality and illegality of the content. It says: “We hold the position that there is no unlawful or illegal content. Sometimes the information that they want to hide about the various public figures, is information whose free existence is undesirable for various corporations. Yes, we’re talking about freedom of speech and expression. But there is a network of ethics. We do not (!) Like spam, carding, phishing, child pornography. All this makes the network better. For posting such material we scroll you without warning. It is also an occasion for the trip is the lack of payment for the services of hosting, or a court decision in the country where the materials are placed (hosting included in the jurisdiction of another country)” The statement reflects the political position of the body which is clear about both the online environment it endorses and the nature of activities it does not support. The activists from this body declared in 2013 that their new hosting site would block visitors from IP addresses that belonged to government agencies and other state

[18] Web hosting is a service that allows individuals and organizations to make their website accessible via World Wide Web. Companies that provide web hosting services actually provide space on a server owned or leased for use by clients and provide internet connectivity in a data center (i.e. a facility used to house computer systems and associated components such as telecommunications and storage systems)

bodies. The reason for the move according to the activists was that ‘the deteriorating state of freedom of information in Russia demanded immediate’. Their aim was to make a plan to ‘clean the web of parasites’. So, they planned to block those IP addresses that were with state agencies and pro-copyright organizations. The main target of this move was Russia’s Safe Internet League (RSIL) (RT 2013). RSIL is an NGO in Russia that is working to make online content as safe as possible for children. Its CEO Denis Davydov was once quoted as saying: “Leading psychologists and psychiatrists should participate in developing requirements for video content hosted on the so-called child friendly version of YouTube in order to eliminate the risk of a ‘wolf in sheep’s clothing”. Far from all videos that may seem harmless to us are necessarily suitable for children (ITAR-Tass 2015)” In 2013, the RSIL had announced an agreement between itself and governor of the Kostroma Region and all 29 internet service providers to conduct an experiment that was termed ‘Clean Internet. This program was meant to limit Internet users’ access to websites and to require personal details if inquiries for controversial content were made. The aim was to provide access only to ‘white lists’ (RT 2013). The case shows that protests to defend right to freedom of expression and access have even fallen out with some interests that seek to protect children. Cyberspace is a vast space with many using it for meeting myriad demands. The kind of clash seen in Russia is a sign of coming of age of cyber politics in which several actors with online interests contend for space. This however also implies trouble in finding a consensus on cyberspace governance.

3.4.1 Political Blogging in Russia

Blogging is quite common among Russian activists. It is also popular among bureaucrats, politicians, mayors, governors and district heads. Although the blogs of bureaucrats are not regarded very lively in Russia because like their job, their blogs are also mundane, they are used for making public some important official information. The incumbent Prime Minister Medvedev is considered a prolific blogger in the country. But there are many other popular Russian bloggers as well. Quora.com, a popular site, has a question: ‘Who is the most famous Russian bloggers?’ It turns out Alexei Navalny and Pavel Durov are regarded as most popular bloggers by some. Other names that seem to be in the mind of the Russians are ArtemyLebedev, RustemAdagamov, Ilya Varlamov, Alexander

Podrabinek, LinorGoralik, Ilya Birman, Anton Buslov, Dmitry Chernishev, Leonid Kaganov, Max Katz and Igor Shiplenok. The links given to their blogs show that for some reasons, Russian bloggers find LiveJournal quite popular for blogging. It is not the names that matter in case of Russia but the platform that is popular among them and what that has done to the way people in Russia consume and circulate news. LiveJournal.com is the most popular online platform among Russian political bloggers. Alexei Navalny also has a blog in that and almost all the Russians mentioned here also have their blogs in the same site. LiveJournal.com is however not Russian in origin. It was created by Brad Fitzpatrick who specializes in computer sciences and started as a web and online community site which built personal journals in March 1999. Later, it was acquired by American company Six Apart in 2005 (www.livejournal.com/support/faq/4.html). This community soon saw its popularity soar not only in USA but also in Russia. The Russian market became attractive when it was found that Russian LiveJournal community was second only to that of USA and had become synonymous with blogging in Russia. Therefore, Six Apart entered into a licensing agreement with international media company SUP in October 2006 that permitted the latter company to manage LiveJournal in Russia. However, just after one year of this licensing agreement, Six Apart decided to completely sell the website to the SUP on the basis of expertise and enthusiasm that latter brought to the branch in Russia. According to the owner, SUP had been successful in doubling the number of users in Russia (Six Apart Press Release, December 3, 2007). Russia indeed has become very vital part of LiveJournal. In 2011, Russian users who use the site celebrated the ten years of its first Cyrillic post. Until that year, there were around two million users of the site. According to prominent media entrepreneur Anton Nossik at that time of the anniversary, LiveJournal had become more than the social networking site. In his opinion, it had become a news site which the news readers were increasingly turning to (Kovalev 2011). A year later, BBC’s Robert Greenall referred to the site as ‘Russia’s Unlikely Internet Giant’ and it is not some ordinary giant. It has become a zone of political bloggers. In 2012, Vladimir Putin was once again standing in the Presidential elections. That was the third time he was standing as a candidate and the step of the Russian leader had miffed quite a number of Russians who felt that they had been taken for a ride. A liberal opposition group did a daring stunt. It hung up a massive banner across the river from the Kremlin, with the face of Putin crossed out and the words “Putin Leave”. The banner was removed but by that time it had started getting circulated in social media through blogs. Millions were able to see the sentiments expressed in the banner thanks to many active bloggers like Ilya Yashin who was the group’s leader. Since its introduction in Russia, people have adopted it with gusto for airing their political opinions. There are other instances of political activists getting real muscles from the blogging sites. Oleg Kashinwho criticized the powerful ones in Russia, was attacked right outside his house. He was almost killed by the attacks that involved metal bars. This news spread in the blogosphere and a protest was held against the ghastly attack. Most of the protesters were those who had no history of street protests (Greenall 2012).

There are three important points that emerge from these instances. Firstly, blogosphere has emerged as a tool of the activism. It is easy to mock the system or authorities in blogosphere where there are million viewers than following rigmarole of the bureaucracy that would not entertain any dissent. Secondly, the blogs have stirred even those people who would have preferred to sit back and were indifferent in terms of action. The circulation of photos and videos can stir people into action, even prodding people to stand and save country from the ruling political class that has become, in their opinion, a symbol of shameless power brokering and corruption. Thirdly, blogs have emerged as alternatives to the official outlets of information. After all, the Oleg Kashin news could not have had received the kind of coverage from official news outlets that the blogs gave it. The victim was able to garner the sympathy thanks to the quick action of several bloggers and it was the sympathy that drove people to come out to protest. This is the Russia of today, much different from its days of limited sources of news. In fact, blogs have enabled Russians to not just consume information but also circulate news. Millions in Russia like billions others outside Russia, have got their moments of agency in which they do not wish to take anything official on its face value. In this context, it is important to refer to the cyber libertarian literature. The way blogs have turned out in Russia, the cyber libertarians have been vindicated. Cyberspace truly has emerged as a space which is liberating. When millions of Russians get to see and write and circulate that was denied to them for long due to either absence of internet or official suppression, the cyberspace becomes a space of liberty. This change is starkly visible because such things are happening in a country that is still more or less ruled by people who are thoroughly of security mindset. It is not that blogs have not played any role in other countries especially countries that have different systems. But they have played the role that cyberlibertarians have been referring to for long. How does all this matter for the cyberspace governance? States have a stake in governance both as beneficiary and as one who can make rules. That kind of rule is indeed powerful one. Apart from state, such a role is available only to non-state actors who have resources and large presence in minds of people. Internet giants can sway sentiments and influence the way they swayed people against the American legislations of SOPA and PIPA. It is important to remember the role played by the tech and internet giants in USA that espoused many of the causes that cyber libertarians cherish: the freedom and innovation. The world's most powerful country that does not baulk at protecting intellectual property rights had to shelve the plan of legislating on the issue under the popular pressure that was led by very visible presence of big players in internet industry. Therefore, this is a tussle in the cyberspace governance that is being played in Russia too and by virtue of that cyberspace governance is not something that concerns the Kremlin. It has other stakeholders as well who may have a different take on how the cyberspace ought to operate. While talking of any Russian approach to cyberspace governance, it is therefore not just the governmental approach that has to be looked at but a set of approaches that have provenance in different values and business models. Former Vkontakte founder Chief Pavel Durov, for instance, was operating a social media platform that inherently allows people to share as well be free. So, it was natural for some uses of Vkontakte to collide with some copyrights stakeholders as well government of the home country of the company. The same is the case with political blogging. It surely becomes a potential threat to the way information is being created and circulated among people. It has an impact on how they would perceive their government. A sight of a beating of an activist will certainly not be viewed very kindly. That is the reason why young people have expressed their revulsion to the way they are being taken for a ride. So, for the bloggers and for political bloggers particularly, the cyberspace governance may not deserve very approving glances if it means laws that restrain the core of their activities: the freedom of expression. The government that faces heat from them however would think just the opposite. Russia therefore has conditions where the needs of various players can be divided into diametrically opposite positions even politically.

3.5 American Internet Giants in Russia: Facebook, Google and Twitter

In present times, if there are three companies that have wide appeal in the international arena in internet industry, it is the three names: Facebook, Google and Twitter. Social media and information search have become a habit among people thanks to these three companies. The new habit of people of course is what these companies have ridden on to success in a number of countries. But certain markets can be quite a tough nut to crack. Russia has been one of those tricky fields in which the play has been competitive and not an easy ride for these companies. In social media, Facebook entered the Russian market in 2008. Vkontakte, the Russian homegrown social media company had established its platform two years before that. Russian market was envisaged in the Facebook's scheme to make inroads in the Eastern market. The market is Europe's largest internal market with as many as 78 million online citizens. Around 82 percent of Russians are present in at least one social network. The people of the country are also known to spend on average 12.8 hours per month on online social networking. After introduction of its Russian language interface, Facebook has been gaining increasing Russian users and traffic. For instance, in 2010, the number of users in the country rose by 376 percent. Most of the users of the social networking site are primarily Moscow based IT, PR, marketing and media professionals who have international friends. This is therefore a highly confined group which consists of fraction of total number of users in Russia. Facebook lags behind the homegrown Vkontakte. The Russian competitor has some features which Facebook does not offer. For instance, Vkontakte allows its users to watch and listen to music for free and allows uploading and downloading video and audio files. These are very attractive features because music and video induce users to spend more time than they would in the absence of such features. The music downloading feature prompts users to keep Vkontakte in the background while working on something else during internet sessions. Facebook does not have this to offer to the Russians (Zinovieva 2014). Apart from these reasons, the reason for the challenge in cracking the Russian market is the late entry of

Facebook's business in the country. During the crucial two years, the homegrown social media platform was able to gain a foothold and develop its brand. Social media has grown rapidly since dawn of the social media companies but late entry means need to share the market with the older player. That is the case of Facebook in Russia. This is however just the business aspect which looks at the pie that Facebook has in its account. There are other problems as well which have dogged the company ever since it entered the Russian market. It has faced pressure from Russian Federal government to remove certain contents from its site or to block some other. It is important to see that Arab Spring saw very crucial role of social media platforms of Facebook and Twitter. The political activism in these sites provoked people to think and act against the autocrats and did enough to create conditions of rebellion. The American tag that these companies carry makes them even an object of suspicion. So, in 2014, when Russia introduced new rules of establishing servers inside the country, the three companies that faced the rod of discipline included Facebook, Gmail and Twitter among several others. These three were asked to register as organizers of information distribution. This meant maintaining a list and records of the user activity for a period of time on servers situated in Russia in order to enable the government to access it (Oliphant 2014). Then later in the same year, a political controversy arose forcing Facebook to give in to the government's request. Alexei Navalny, the blogger and activist who is main opposition leader and a strong voice among anti-Putin critics had been in jail since 2013. His supporters developed an event page in Facebook to organize demonstration in his support in 2014. But the company blocked that page after facing pressure from Russian government to do so. The event page had attracted 12000 prospective participants in the planned event. The supporters of the opposition leader were disappointed with the action of Facebook. They were "very surprised" and "very disappointed" to see the promptness with which Facebook complied with the government's request. The company also looked inclined to avoid the controversy altogether as its spokesperson refused to comment on the grounds that it was not the policy of the company to discuss specific blocking case. To the surprise of some users, similar pages that were promoting anti-government events were not blocked. One page which was almost a clone of the page that had been blocked had been spared. It was curious in the opinion of many users that this latter page had gained 25000 prospective participants. According to some internal source, Facebook had actually received many more requests targeting other pages as well but the company had not acted upon all the requests (Roth &Herszenhorn 2014). Later when many more requests started pouring in, the company left the pages totally untouched. This inconsistent approach has been attributed to the dilemma the American social networking companies face when operating in a different political milieu than the one which USA has. While operating in a different territory, the market considerations have to be taken into account because they are the reasons for entering the country's market in the first place. On the other hand, compliance with the requests that are aimed at squashing any expression of dissent is seen as damaging reputation among users and against libertarian ethos that flourish in Silicon Valley. Facebook's initial response to the Russian government's request was even criticized by the US ambassador in Moscow, Michael McFaul. When Facebook blocked the page on December 20, the ambassador wrote in his Twitter account: "We all make mistakes. @facebook should correct theirs in Russia asap. Current action-horrible precedent and bad for business". Facebook did not put any up any response to the ambassador's remarks. But Russian official apparatus took note of it. Russian parliamentarian Mikhail Degtyaryov told the Russian news agency: "McFaul should be quiet and Facebook should obey Russian laws. We know what happens to countries that don't limit extremist activity online-that's the Arab Spring…Russian doesn't need that" (Schechner& White 2014). The remarks made by the Russian parliamentarian at a time when countries in Arab world are experiencing violent upheavals are indicative of Russian take on the Facebook and Twitter revolution. For several others, the kind of social media provoked rebellions may be more fantasy than substance, but Russian officials do see the reality in that. Facebook has to be conscious of this fact even as it does business in the country. It may have arisen in libertarian and free milieu but as an Internet behemoth with several users, business comes first. Not doing so makes it vulnerable to the barrage of suspicion based pressures to block just any page that is only remotely connected to any protest. This thing apart, any involvement of American official even in the form of reaction actually makes the business part difficult. Therefore, any comparison of Facebook with Vkontakte will not be complete with just statistical data that reveal their market share and growth in Russian market. Vkontakte, for all its support to the anti-government protests and the libertarian talk by its former chief Durov, is still without the American baggage. The remark made by Russian parliamentarian referred to Arab Spring, leaving out any reference to Vkontakte’s vibrant dissent pages that encourage people to come out on the streets. The message was therefore clear: fall in line to respect our sovereignty. In 2015, it was reported that the head of Russia’s media watchdog Roskomnadzor, wrote to the heads of Facebook, Google and Twitter, and accused them of committing ‘lawless actions’. The companies were threatened with fines, bans if they did not act swiftly to block content that the Russian authority deemed extremist. According to the spokesperson of the media watchdog, such letters were part of standard practice in the communication with foreign Internet companies. The watchdog also asked companies to provide information about the number of visitors to specific pages (The Moscow Times 2015).

Google’s case is not very different either. In terms of competition, it faces a tough Russian rival in Yandex. Yandex, as a company, is however registered in Netherlands. In 2002, Yandex established itself as the leader of the online search market in Russia, leaving far behind its competitors Mail.ru and Google. But that was then in 2002. Google was only one year old then, as the search engine behemoth had entered Russia only in 2001. It established its Russian language morphology based search capabilities only in 2006. But it began to make inroads in the mid 2000s when its aggressive approach took its market share from 6% to 18% and that of Yandex fell from 60% to 51% (East-West Digital News 2011). So, Yandex began to take its distant rival seriously. In 2012, it introduced new browser to take on the challenge posed by Google Chrome. Speed is the main feature in browser competition. Yandex’s new browser promised to be as fast as Google Chrome. Apart from this, Russian search engine also bought a license for 40000 Android applications from Opera which allowed it to open its own worldwide Yandex Store. The company soon started negotiating with hardware manufacturers to have Yandex Store pre-installed on tablets and smartphones instead of the Google Play. The Store will integrate Yandex.Music, which is a mobile music shop and Yandex.Money which will provide alternative to Paypal and Yandex.Maps seeks to give competition to Google Maps (Hermans 2012). The seriousness with which Yandex is going about to offer alternatives to Google implies that it is quite cognizant of the potential of the Google to make a dent on its market share in its home market. However, Google did not have it easy. It has been facing the ire of the anti-trust complaints. The episode discussed earlier, has given bad publicity to the company. This however is not the only rough patch in the journey of Google in the country. The Federal Government of Russia feels that the search engine is not coughing up enough tax amount and so new laws are being contemplated to ensure that foreign companies like Google and Apple pay enough taxes (The Moscow Times 2015; Sawers 2015). ‘Enough tax’ is euphemism for extracting more amounts out of them. Twitter as opposed to Facebook and Google is not talked about much in controversies. But the story is not very different here either. Twitter like any other micro-blogging platform has been gaining popularity in recent times. According to a Semiocast information posted by Ana Oshkalo, Russia ranks 14th in terms of Twitter usage. Earlier, Russia’s ran was 20th. The climb took place in just few months. According to search engine Yandex, the Russian speaking audience of Twitter crossed 1 million mark in July 2011. Six months later, Yandex’s Twitter rating included 1.68 million accounts. Vedomosti.ru, a major Russian newspaper argued that much of this growth took place during Russian Parliament elections (Oshkalo 2012). But this growth has not gone without getting noticed by the authorities. In information revealed by the company, Russian authorities had demanded information on 108 requests pertaining to the viewership of certain blogs. The company stated that it did not give the information (Razumovskaya&Schechner 2015). This has not been very different from the experiences of other social media companies in Russia. Each company had had its unique experience but the similarities are too many to be ignored. They are: contending with a very well entrenched security bureaucracy.

3.6 Spinternet in Russia

There is a predominant presence of cyberlibertarian opinion that cyberspace is a zone that ought to be free and is in fact a free zone that promotes freedom of speech and provides liberating experience. But this perspective appears to be shadowed by the way certain regimes are using cyberspace. According to EvegenyMorozov, several dictatorships have been aided by cyberspace. People in the dictatorships who are well versed with the cyber technology have used Internet to hunt down the dissenters and propagate their own ideas. This has enabled them to not only survive but also conduct their propaganda to counter the dissenters. Morozov has called it ‘spinternet’. The term is a combination of ‘spin’ and ‘internet’ which means to spin the internet (Millar 2010). Spinning the internet means creating a presence in the cyberspace to show the regime in kinder light than what might exist in the absence of such presence. This can be done best through blogs and social media platforms. These blogs are often said to be fake and paid ones. It has been found in an investigation that Kremlin indeed uses a troll[19] army to get the spinternet job done. This troll army consists of paid bloggers who allegedly work round the clock to flood the Russian internet fora, social networks and comment sections of western publications with remarks that praise Vladimir Putin. The same are also paid to rant against the unjust behaviour of the west. These trolls are paid handsomely but are fined for being few minutes late or for failing to reach the required target. According to an unnamed troll, the comments included the interspersing of political comments with the ordinary ones. For instance, a blog in LiveJournal included posts about the Europe’s 20 most beautiful castles and signs that show that you are dating the wrong girl. These posts are mixed with political comments on Ukraine and Russian blogger Alexei Navalny that say he is corrupt. The posts are meant to show the west in poor light. For instance, Barack Obama is shown as monkey eating bananas, and Ukrainian President Petro Poroshenko in drag declaring: “We are preparing for European integration”. The information given along with such posts are given links to a site called ‘patriotic Russian Wikipedia’. According to this Wikipedia, the Euromaidan protests in Ukraine had all protesters who were fed with tea laced with drugs. On the other hand, everything is done to show Vladimir Putin as better than his western counterparts. As an example, Putin is shown as a man of peace and as someone who has been fighting against extremism (Walker 2015). Similarly, when opposition leader Boris Nemtsov was killed, trolls flooded the internet with comments that showed that he was actually killed at the behest of Ukrainians because he had snatched away one of their women. Nemtsov’s girl

[19] Troll is an Internet slang, which refers to a person who posts comments, pictures or messages in online communities (newsgroup, forum, chat rooms, blogs) with intent to provoke emotionally charged response from the people who are targeted. The activities of troll often cause discord and even harassment to the person who is being targeted by the troll in comments. Therefore, it has been associated with online harassment also recently. Trolls have been found to target big personalities and celebrities because they have huge following and it is easier to cause disruption in such cases.

friend who was with him at the time of his killing is Ukrainian. The comments were spread in a network that was very close knit and quite dense and appeared to be growing (Alexander 2015). Paul Roderick Gregory writing in Forbes has called the alternative world created by trolls as Putin's Alice-in-Wonderland. In his opinion, Putin has used trolls extensively to create a perception favourable to him and this has been going on unnoticed even before the Crimean annexation. If people are trying to access on the Ukrainian problem and type the key words, the job of trolls is to flood the internet with stories that say that it was the Ukraine that attacked Russia (Roderick Gregory 2014). The trolls have been active in the comments section of the western news outlets like Guardian, Fox News, the Huffington Post, WorldNetDaily, Politico and the Blaze. There is allegedly important role of Nashi[20] brigade in this trolling according to the readers. The reaction of western media to the alleged trolling by Putin's paid troll army has been to parody him in every sense, making fun of his media appearances. As an example, the *Daily Show* by Jon Stewart called Putin's behaviour that reflects not the leader mentality but a 'toddler mentality'. The show attempts to punch holes in the media hysteria created by the Putin's shirtless appearances by mocking the whole thing through caricature. Putin is also said to have appeared hunting or posing with big tigers. The show reveals that the supposedly hunted tigers are first tranquilised for Putin; making mockery of the Russian leader's forest expedition (McKenzie 2014). It has been noted that the Russian leader has been a sporty type but the troll story that has reached the internet and especially western media outlets has attracted a counter campaign in internet.

3.7 E-Commerce in Russia

[20] Nashi Brigade is a short name for Molodezhnoyedemokratichcheskoyeantifashistskoyedvizhenye "Nashi" which translates into Youth Democratic Anti-Fascist Movement "Ours". So, the name itself declares its aim which is to fight fascism. It is said to have been created after encouragement from Russian Presidential administration under President Putin's term. By 2007, it had grown in size to the membership of 120,000 persons in the age group of 17-25. It is said to have divided in 2008 into four groups: Nashi 2.0, Steel, All Houses and Nasha Victory. In 2012, it was even announced that movement would be dissolved to be replaced in future by a new organization. The reason stated was that "movement had been compromised" during the recent Presidential election.

E-commerce is the one of the fastest growing areas of internet based businesses these days with several countries having domestic players in addition to the American giants of e-Bay and Amazon. China has got Alibaba that is establishing its hold in other countries and India has now many e-commerce players. Flipkart, Snapdeal, Lenskart, JustDial are just few names in the crowded Indian e-commerce market. Russia has also caught up the e-commerce trend and it has its domestic players catering to the consumers. There are some data that throw light on the emerging nature of the business in Russia. A report by East-West Digital news called E-Commerce in Russia says the following:

1. Around 30 million Russians went for online shopping in year 2013. This had twenty three percent of the population of age eighteen and above.
2. E-commerce still consists of small merchants and is largely fragmented. According to the report there are fewer around 39000 internet shops but fewer than twenty earn at least $100,000 a year.
3. The growth rate of the market is 20 percent a year (East-West Digital News: 14-16).

The other data by research firm Data Insight says that e-commerce revenue in 2013 was $16.5 billion. This was a 28 percent increase from 2012 and constituted two percent of total retail expenditures. Also, consumers in Moscow and St. Petersburg constituted 30 percent of internet users but made up 60 percent of the online shoppers in Russia (Kaplan 2014). In terms of discounts and prices, Russia has been costlier than US and other western countries. It has been found that this is due to inefficiencies and reliance on Russian Post whose delivery services are slow and not up to the mark. Sometimes, the Post loses the parcels. The limited statistics here show two things. Firstly, e-commerce as a segment of retail trade is still developing and has not reached the level where it forms a major chunk of retail purchase. Secondly, it does not look very widespread geographically. If Moscow and St. Petersburg give sixty percent of online shoppers, then it implicitly means that other cities in a large country like Russia are contributing miniscule amounts.

The important players in the Russian e-commerce market are Ulmart.ru that deal with wide range of things (from electronics to home and garden appliances) and

Ozon.ru. The turnover of former in 2013 reached 420 billion euros in 2013 that excluded Value Added Taxes and offline sales. Ozon is seen as Amazon of Russia while other players are KupiVIP and Biglion (Ecommerce News 2014). Conducting shock sales is common among e-commerce players. This is done to beat sales records and attract maximum number of users to the website within 24 hours. In March 2015, KupiVIP.ru announced a one day shock sale. In this, the company announced that many branded products would be available at a considerably reduced price and brands were from ten different countries. To attract the customers, the brands that were featured included Karl Lagerfield, Galiano, Prada, Dolce & Gabbana, Alba, Top Secret and Marcobonne. According to the company, 89 percent of its buyers love the global one day sale format because they expect interesting offers on such days (Ecommerce News 2015).

Russia has been important market for many European e-commerce players but a gradual shift is taking place. The European players have ceded space to the Chinese e-commerce companies. This has been attributed to the devaluation of ruble. The fall in Russian currency in 2014 was considerable, amounting to 40 percent. Since currency fluctuations directly affect the price, the Russian consumers have been turned off by high prices. This was accompanied by a jump in the share of Chinese e-commerce players. In 2014 70 percent of packages to Russian consumers from abroad had come from China. This figure was only 40 percent in 2013. But European brands are still popular in the Russian e-commerce market (Ecommerce News 2014)

3.8 Conclusion

Cyber crimes are one of the biggest challenges that Russia has to face in the realm of cyberspace governance because it has a direct bearing on how it would be perceived by international community. In this, it faces the challenge of curbing the internal ecosystem of cyber crimes. The second area that has created challenging situations is the increasing cases of clashes between several internet and social media companies and copyright organizations. The non-state actors, primarily private entities are divided on this with both pro and anti-copyright organizations voicing their concerns about the cyber laws. This requires a fine balancing act by lawmakers in Russia. It is however the increasing uses of blogs and social media platforms for political activism that has the government worried. This has come at a time when role of social media channels of communication in instigating and strengthening Arab Spring protests has been noted. There have been numerous instances of uses of blogs and social media in which the authorities were defied and challenged, resulting in clashes and coming out of protesters in Russia. Since, political instability is a spectre which Russia does not wish to be realized for reasons of security, the role of social media companies and the activities they promote are bound to come under scanner during making of cyber and information laws in the country.

4.1 Introduction

The emergence of certain areas of cyberspace has become important in shaping cyberspace governance issues in. These are the spread of internet activism through social media particularly blogging, increasing cyber crimes with transnational links and of cyber networks of paedophiles, intellectual property infringements due to new platforms of sharing, cyber surveillance with transnational effects and active use of the cyberspace by the governments. These form the focal area. There are various opinions on these, coming from both state and non-state stakeholders. So, Russia and several non-state actors in it are dealing with unsettled questions. This has given rise to jostling for leadership. That is happening among state actors anxious to have control over a new sphere. Russia finds itself amidst this contentious environment where it has to propagate some kind of model of cyberspace governance even if it is a little vague. The benefits of doing so are huge considering the economic and political benefits it would accrue while avoidance carries the risk of being sidelined in an important global discourse. Therefore, Russia has been seen actively pursuing the cyberspace governance issues. In doing so, Russian position has been playing an important role in changing the way internet is controlled. It has been championing the international control of internet. Internet and control sound like oxymorons because internet has been widely understood as one that has evolved on its own and has been so for practical purposes. The Russian perception has been different from this one. Russia’s constant refrain has been that it is now important to take the control of internet from one country (referring to USA) to a more dispersed international control. Therefore, apart from the domestic issues of internet, the internet governance discourse in global fora has been an important factor in giving sufficient inputs to form an approach to the governance issue. In this, it has found quite a number of allies giving it an opportunity to assume the leadership role in global cyberspace governance. The recent revelations by Edward Snowden have accelerated the speed with which Russia is pursuing this. In this context, Russia has taken up a number of bilateral and multilateral initiatives to formalize cyber security discourse. Cyber security discourse has so far included many cyber attacks that have taken place with a lot of attention being absorbed by the alleged role of state actors. In recent times, Russia has been marked out for its potent attacks on cyber systems of a number of countries. So, cyber security dialogues that Russia has been involved with, have involved making some kind of alliance against status quo which has a western perspective. Since, this has a direct bearing on how a state controls cyberspace, it forms an important part of the state led approach of cyberspace governance.

4.2 Current Context of State Led Approach

The discourse on cyberspace is gradually ceding space to increasing the role of state. As opposed to the earlier years of development of internet, a lot more now happens because of state led and state run activities. In this, three state led activities have emerged. They are:

1. The State Surveillance Activities
2. The Cyber Diplomacy that involves the bilateral and multilateral efforts to govern cyberspace
3. A Legal Approach to cyber activities to control it domestically.

There are no clear cut divisions that separate them because they are connected with one another. However, they are emerging as three different areas that states are now handling with discrimination. Russia as a state actor too has to discriminate between the three because however connected they may be, they require different ways to handle.

4.2.1 State Surveillance Activities

Surveillance activity of a state is itself an act of cyberspace governance. This is because of the total involvement of the cyber infrastructure that a country has command over in doing so. The recent revelations of NSA snooping have shown that surveillance is not an activity that a government machinery can do alone. It requires a lot of collaboration, participation of other non state actors to fulfill the goal of surveillance. Governments can mastermind the surveillance while it is the other actors who have to often do much more than known, to complete surveillance. But the overarching presence of state looms like a shadow that is possibly the reason why it has been called the state surveillance and not something else. The other reason is because it is the security aims and goals that the activities fulfill. The collaborating non- state actors play supporting role to realize those goals. For instance, in the NSA snooping, surveillance was the interest of the US government but crucial supporting role was played by the tech giants like Facebook and Google in making that happen. This is not very different from what is happening in some other countries that have been known to do the same. Cooperation of social media companies in keeping tab on anti-state activities are commonly sought in Russia, China, India, Iran and Saudi Arabia. So, the US actions are not out of place or entirely novel. However, they have brought out into the open what states have been doing to use cyberspace to meet their ends. Surveillance activities that have been noted and reported bring out how states have adapted themselves by exploiting a new medium to do age old activities of keeping a tab on friends and foes. Cyberspace therefore becomes a new instrument and in the process has got co-opted by the state structure. So, surveillance is governance through developing the instrumentality of cyberspace. The instrumentality ensures that cyberspace gets disciplined. So, the NSA revelations made by Edward Snowden gave shock to some state actors due to the fact the US actions appeared to be developing this instrumentality to a new level. This new level was seen as the potential harbinger of a shadow of a powerful actor with ability to reach any corner of cyberspace. It is quite similar to the Orwellian concept of Big Brother watching[21]. So, the strong reactions were more due to this Orwellian presence that states felt could erode their sovereignty. It was the question of protecting one’s information sphere which could not be left at the mercy of the instrumentality of cyberspace of another state. In this context, the Russian reaction was measured. The Russian President said when asked about the surveillance question that his country was not new to surveillance but there were set laws to enforce them and enough was done to ensure that it was done within a legal framework of the country. In 2014, Snowden asked Putin question about the same in latter’s annual question and answer program via a video link. He asked whether Russia intercepted, stored and analyzed in any way the communications of millions of individuals. He also asked him whether he believed that simply increasing the effectiveness of intelligence or law enforcement investigations could justify placing societies rather than their subjects under surveillance. Putin’s response was that Russia had special service that bugged telephone conversations

[21]

and Internet communications to fight crimes including terrorism but only with court permission and for specific citizens. He however denied that Russia's surveillance had a mass character. He said: "On such a mass scale. We do not allow ourselves to do this, and we will never allow this. We do not have the money or means to do that." (Watkins 2014). The views expressed bring out Russia's understanding about the inevitability of using cyberspace as an instrument to meet goals of states that they regard fundamental to their existence: their security. What he also meant to point out was that if done within the sovereign borders and laws, surveillance was not an activity that could be avoided. The mention of cyber crimes and terrorism particularly highlighted that Russian leader did not think it proper to paint all kinds of surveillance with the same colour. Therefore, the aim of Russian President's remark was to make it obvious that his country had wherewithal to be discriminatory in surveillance but could not consider the surveillance of mass nature. Russia has also taken a number of actions after the Snowden episode in surveillance to boost the country's security.

4.2.1.1 Russia's SORM Series of Surveillance

Russia's surveillance has been under SORM series of system. SORM is an acronym for the Russian term which translates into System for Operative Investigative Activities. SORM-1 was established after passing a law in 1995 that allowed Federal Security Service (FSB) to monitor telephone communications. SORM-2 was established in July 1998 to allow monitoring of internet in addition to telecommunications. This SORM is said to mandate Russian Internet Service Providers to install special device on their servers to allow the FSB to track all credit card transactions, e-mail messages and web use. This device whose cost is in the range of $10000-$30000 has to be installed at the expense of ISP. Some ISPs were also said to have established direct communication links with FSB that cost even more than this amount. In July 2000, the surveillance task was further facilitated by issue of Order no. 130 by Ministry of Information Technology. The order was titled 'Concerning the introduction of technical means ensuring investigative activity in phone, mobile, and wireless communication and radio paging networks'. It exempted FSB from providing telecommunications and internet companies the documentation on targets of interest prior to accessing information. Then from April16, 2014 onwards, new requirements for wiretapping were introduced under SORM-3. Under SORM-3, telecommunications operators are required to install compliant probes (Wikipedia.org). During Sochi Olympics, the surveillance was found to be extensive by number of countries. Soldatov and Borogan (2013) write that US State Department issued warning to Americans who were desirous of coming to watch Sochi Olympics and asked them to be watchful about SORM. They issued the list of Travel Cyber Security best Practices that was quite long. It included among taking actions like sanitizing the essential devices, turning off the Wi-Fi, avoiding connecting to local ISPs at cafes, coffee shops, hotels, airports or other local venues etc. This was in reaction to what was seen as tight Russian surveillance. Anyone who wanted to watch Olympics in Sochi required a spectator pass. This pass could be had by registering on the official Sochi Olympics site with the photo and requested access to camera and microphone. The writers further explain the vast extent of control of FSB over the surveillance and the ease with which it can be done. This system which is now widely called SORM, the authors argue, is a holdover from the Soviet past. FSB has control centers that are directly connected to operator’s computer servers and any internet communication can be accessed by FSB agent by entering a command into the control center located in local FSB headquarters. So, the Russian surveillance has FSB playing an important role in the system of SORM. In early 2000, however, President Putin introduced a legislation that allowed seven more law enforcement and security bodies to have real time access to e-mail and other electronic traffic (Tracy 2000).

4.2.1.2 Roskomnadzor

The main agency for surveillance on internet is Roskomnadzor. Roskomnadzor has a vast functional area and is not confined to internet surveillance. But its important functions are performing state control and supervision through compliance with the legislation of Russian Federation related to mass media and mass communications, television and radio broadcasting. It also looks at the compliance with the requirements for telecommunications and postal communication networking, and with the requirements for design, construction, renovation and operation of telecommunication networks and facilities. In early 2015, the chief of the body A. Zharov spelt out certain priorities in which a lot was about information security (Federal Service for Supervision of

Communications, Information Technology and Mass Media, April 20, 2015). He pointed out the following:

1. Work must be continued to enhance the stability and information security of Russia's public communication network which would include development of a system to monitor telecom service quality.
2. Work to counter the use of news media and the Web for extremist activities is also a priority. Zharov said: "Information acts aimed at destabilizing the country cannot be ruled out, so we should improve and make effective use of all legal methods and means of countering extremist acts in the media.
3. It is also important to extend the scope of anti-piracy laws to include books, music and software products and Roskomnadzor is all set to cooperate with the Web user community in the new areas of protecting intellectual property rights in the Web.

So, information security is the topmost priority of Roskomnadzor even as it deals with myriad other issues related to internet like intellectual property rights protections. It has been found that intellectual property rights violations have become rampant due to new ways to share information and entertainment services. Zharov's talk of intellectual property protections in Web also balances the hard talk about the use of web by extremists. So, it also reflects that the agency is equally concerned about the role that it has to play in the changing technological scenario where it might have to tackle the problems arising out of old systems of knowledge creation and new ones in the internet. The priorities are also indicative of the composite nature of the role of the agency. It is an overarching body that seems to be dealing with everything. In nutshell, Russia already has a robust surveillance system and due to that the country is not likely to take a total stand against cyber surveillance as long as it remains within the sovereign limits. None other Russian President has indicated that.

4.2.2 Cyber Diplomacy

After cyber warfare, cyber security, cyberspace governance and cyber weapons, cyber diplomacy is the new development. It is the thread that runs through all the above mentioned terms and is closely connected to all bilateral and multilateral efforts to increase the role of state in controlling cyberspace. Several multilateral efforts have been taken at WSIS, UN and a few cyber conferences. Bilateral efforts have also picked up and have grabbed many more eyeballs than multilateral. Both are playing a role similar to the negotiations on climate change. There are stark differences and both multilateral and bilateral efforts are meant to arrive at consensus on the fractured discourse. Russia is playing a key role in both

4.2.2.1 Bilateral Cyber Diplomacy

The bilateral cyber diplomacy is the most recent byproduct of the last one decade of evolution in cyberspace. Countries are increasingly facing cyber attacks and some countries have been targeted more than others while few have been found to be source of attacks more than others. United States has been claiming that it has become the top target of cyber attacks and supporting its claims are some of the incidents that came to light. In 2015, United States became target of cyber attacks allegedly from North Korea. Some North Korean hackers had hacked into Sony Corporation’s website and exposed top secrets including confidential conversations between top people of the organization. The attack almost coincided with the release of the movie The Interview. The movie has a North Korean connection. The plot of the movie revolves around a comical situation of a plot to assassinate North Korean leader Kim Jong-Un and Sony Corp was going to release the movie. The hackers who attacked the Sony website warned that there would be 9/11 style attacks if the release of the movie took place. US President called the actions of cyber attacks ‘acts of cyber vandalism’. He later called the initial cancellation of the release of the movie ‘a mistake’ (Grisham 2015). According to the President, the country could not cave in to the blackmails of the hackers. The President also talked of retaliation. After a gap of few days, North Korea experienced cyber systems outage. This was seen worldwide as retaliation to North Korea’s actions. But this is not the only case in which two rival countries have been involved. Two other countries have been branded as the silent attackers who have been making cyber attacks that are of surreptitious type.

According to US, China has been the top source of a number of cyber espionage hacking that was discovered. For instance, US Defense website has been found to be hacked by hackers at least on one occasion and the attack was traced to China (Sanger 2013). Similarly, Russia is also seen as a potent player in cyber warfare scenario. Its attacks on Estonia and Georgia were found to be timed with the conflicts with both the countries that Russia was experiencing. The Estonian attacks came soon after the country miffed Russia by allowing the demolition of a World War II memorabilia. The country was affected and isolated due to DDoS attacks. In case of Georgia, the attacks from Russia were well timed to go parallel with armed intervention in the brief armed conflict between Russia and Georgia. US President took note of the Russian actions in one of his Press briefing later while unveiling US Cyber Command (White House Press Release 2009). US was however more taken by surprise in 2010 when country's stock exchange company NASDAQ's computer system was found with a silent malware. The malware was dubbed as digital bomb. It was traced to Russia. Russia has also been noted for harbouring underground networks of cyber criminals and hackers. The attack could have brought about a collapse of financial system of the country. (Wei 2014). So, Russia and China are two countries that have been noticed in cyber war and cyber espionage activities and have attracted attention of USA which claims to be affected by attacks emanating from these two. Therefore, the most intense diplomatic exchanges and activities have taken place within this triangle of Russia, China and US with Russian and China on one side and US on the other. China-US cyber diplomacy and exchanges are important to understand Russian position because of the Russian-Chinese tango on global fora on several other issues. The need to counter US exists as an unstated factor in cyber diplomacy as well.

4.2.2.2 US-China Cyber Diplomacy

US-China cyber diplomacy began in early part of 2013 when the White House demanded that the Chinese government stop the cyber theft of data from several American computer networks and asked China to agree to an acceptable norm of behaviour in cyberspace. US President Obama's national security adviser Tom Donilon made a speech in which China was publicly confronted over its cyber espionage activities. This was a response to the then Chinese Foreign Minister Yang Jiechi's rejection of growing evidence of his country's involvement in cyber attacks on American corporations and some government agencies. He said:

"The White House is seeking three things from Beijing: public recognition of the urgency of the problem; a commitment to crack down on hackers in China; and an agreement to take part in a dialogue to establish global standards. Increasingly,

> U.S. businesses are speaking out about their serious concerns about sophisticated targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale. The international community cannot tolerate such activity from any country".(Landler and Sanger, the New York Times, March 11, 2013).

In the same year and around same time, US Director of National Intelligence James Clapper had told a Senate Committee that cyber attacks and cyber espionage had supplanted terrorism as the top security threat facing the country. Also, a day after Tom Donilon's speech, President Obama was asked in an interview in ABC News whether the claims by US lawmakers that scale of cyber attacks on American firms and infrastructure amounted to a cyber war with China (BBC News March 13 2013). To this, the President replied:

> "You know there is a big difference between them engaging in cyber espionage or cyber attacks and obviously a hot war. What is absolutely true is that we have security threats. Some are state sponsored. Some are just sponsored by criminals. We have made it very clear to China and some other state actors that, you know, we expect them to follow international norms and abide by international rules. And we'll have some pretty tough talk with them. We already have."(BBC News 2013).

The above mentioned efforts by USA to make China fall in line are important from the perspective of cyberspace governance. Firstly, it has brought out the American perception that cyberspace is no more just a domain where non state actors rule the roost. There are many things that state actors are surreptitiously doing (reference to Obama's "some are state sponsored and some are sponsored by criminals"). The recognition of role of state actors is a significant step in forging understanding on global cyberspace governance. It reflects that there are several spheres that will have to be dealt with head on by states. It also means tighter control of cyberspace by state actors. Obama's remarks also have to be seen in the overall context of increasing need to deal with cyber crimes within a system where states can make diplomatic exchanges. Secondly, the American perception is that there is some 'norm' which has to be followed by China. The mention of international norms is significant because it implies countries taking responsibility for whatever number of cyber breaches and attacks is traced to them. It implies that cyberspace governance has to ultimately take cognizance of how states ought to behave with regard to conduct in cyberspace. Thirdly, the unequivocal reference to China's role in cyber attacks shows American efforts to establish a practice of cyber diplomacy whereby issues of cyberspace like cyber attacks can be dealt with. So, if earlier it was believed that cyberspace was a zone that aided cyber attacks without dragging in the state actors, now the façade has fallen. USA is the first to state that all were not the handiworks of cyber criminals. China initially responded to American accusations by saying that it was in fact the victim of increasing cyber attacks. Chinese Foreign Minister Yang Jiechi issued his own call for rules and cooperation on cyber security and stated that the reports of Chinese military involvement in cyber attacks were built on shaky grounds (Landler and Sanger 2013). This was followed by setting up of US-China Cyber Security Working Group in April, 2013 which had inaugural meeting in July 2013 (BBC News 2013). However, the year 2013 was rocked by revelations by Edward Snowden about NSA global snooping that involved espionage on some Chinese companies and officials. In March 2014, China demanded USA stop snooping activities of NSA against Chinese officials and companies. Chinese Foreign Ministry stated that China was ‘extremely concerned’ that USA’s NSA had infiltrated the servers of Chinese telecom giant Huawei, Chinese Trade Ministry, national banks, leading telecommunication companies and officials of the country. The spokesperson of the ministry said that China had lodged complaints with US in that regard and asked them to stop such acts. He further that China believed that internet communication technologies should be used to develop ones economy in a normal way and not for stealing secret information, phone tapping and monitoring (RT March 26, 2014). This was followed by China’s action of setting up a new government body in February 2014. This body is tasked with overseeing China’s cyber security. At the time of the taking charge of the body, Chinese President Xi Jinping vowed to make China a ‘cyber power’ and compared the twin goals of developing country’s information technology and cyber security capabilities to “two wings of a bird and two wheels of an engine” (Wan 2014). Nearly three months after this, China suspended its involvement in US-China Cyber Security Working Group calling US actions (reference to NSA snooping) “a serious violation of the basic norms of international relations”. A Chinese Defense Ministry statement referred to Wikileaks and Snowden revelations and said that “US hypocrisy and double standards on network security have long been obvious” (Shi and Riley, Bloomberg, May 20, 2014). US had also charged five Chinese military officers with hacking American firms. The same year, Chinese

President Xi Jinping made the remarks in Brazil: “No matter how developed a country’s Internet technology is, it just cannot violate the information sovereignty of other countries” (Jiao and Shengnan 2014). Late in the same year, Yang Jiechi, the state councilor for foreign affairs told John Kerry, the US Secretary of State that US should take positive actions to create necessary conditions for bilateral cyber security dialogue and cooperation to resume, He said; “Due to mistaken US practices, it is difficult at this juncture to resume Sino-US cyber security dialogue and cooperation” (Reuters 2014). So within a short period of two years, USA and China have made number of moves that have had consequences for the nature of discourse on cyberspace. Their diplomatic exchanges go on to show that important players are increasing the role of state in defining how the cyberspace ought to be.

4.2.2.3 Russia-China Cyber Diplomacy

Russia and China are apparently on the same side as far as future vision of cyberspace is concerned. The two have already signed a cyber security pact and it has been perceived as a product of common mistrust of social media and internet induced Arab Spring protests (Leyden 2015). This came after it had been anticipated before Russian President Putin’s state visit to China. It has also been touted as a pact that has solidified their friendship in the new millennium that has seen rise in cyber attacks and cyber warfare increasingly become part of state actors’ arsenal and military strategies. The pact brings together the two countries on the following points:

1. Agreement to not conduct cyber attacks against each other
2. Jointly counteracting technology that may destabilize the internal political and socio-economic atmosphere, disturb public order or interfere with internal affairs of the state
3. Agreement for exchange of information between law enforcement agencies, exchange of technologies, and ensuring security of information infrastructure.

In the introductory note or the Preamble of the Agreement between the two countries, the fundamental understandings that form its foundation are stated. They are stated as follows (See Appendix 1):

1. “Reaffirming that the sovereignty and international rules and principles derived from the state sovereignty, applies to the conduct of States in activities related to the use of information and communication technology, and the jurisdiction of States over information infrastructure in their territory, and that the state has the sovereign right to define and implement public policies on matters relating to information and telecommunications network “Internet.”
2. “Attaching great importance to the balance between security and human rights in the field of information and communication technologies”
3. “In order to prevent threats to international information security to ensure the interests of the Parties in order to create an international environment that is characterized by peace and cooperation.”
4. “Trying to form a multilateral, transparent and democratic international system of management of information and telecommunications network “Internet” in order to control internationalization of information and telecommunications network “Internet” and equal rights of states to participate in this process, including the democratic governance of the main resources of information and telecommunications network “Internet” and their equitable distribution.”

Article 2 of the Agreement lays out the threats to the information security considered in its implementation. They are as follows:

1. Carrying out acts of aggression that are aimed at the violation of the sovereignty, security, territorial integrity of States and a threat to international peace, security and strategic stability;
2. Use of ICT for causing economic and other damage, including through the provision of a destructive impact on the objects of the information infrastructure;
3. Use of ICT for terrorist purposes, including for the promotion of terrorism and involvement in terrorist activities and more supporters.
4. Use of ICT to commit offenses and crimes, including those relate to unauthorized access to computer data;
5. Using ICT to interfere in the internal affairs of States, to violate public order, causing incitement of ethnic, racial and religious hatred, propaganda of racist and xenophobic ideas and theories that give rise to hatred and discrimination, incitement to violence and instability, as well as to destabilize the internal political and socio-economic situation and violation of government;

6. Use of ICT for the dissemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States.

The points included in the preamble and the nature of threats identified for the purpose of the agreement are such that they bring into the traditional sovereignty framework all the cyber activities that can be threat and cause of dispute. In fact, Article 9 of the Agreement is about the dispute resolution between Parties to the agreement (See Appendix 1). At the same time, the parties make it explicit through Article 8 that the agreement is not directed against any third country (ibid).

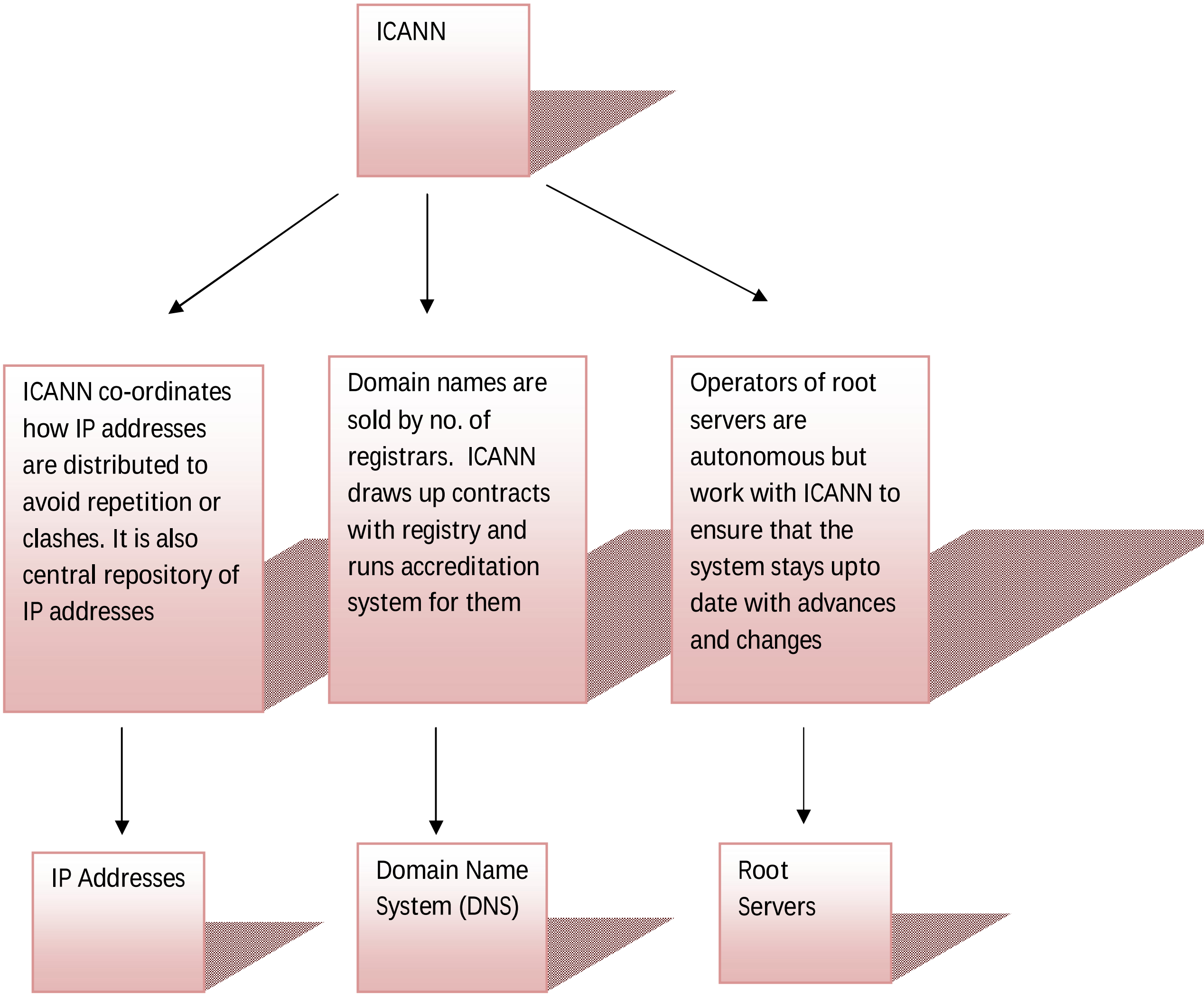
According to Oleg Demidov, a cyber security analyst, the agreement with China to cooperate on cyber security was an important step in terms of pivoting to the East. He said: “The level of cooperation between Russia and China would set a precedent for two global cyber security powers (Razumovskaya 2015). Some voices of concern began to pour in after this pact was signed. Mike Rogers, the former Chairman of US House Intelligence said that pact was “designed to suppress the dissidents”. According to him, it was to facilitate theft and to conduct aggressive actions in neighbouring countries. He further said: “The implications of this are really quite concerning”. He also questioned whether China and Russia would get sucked in on the cyber front to one another’s regional disputes and stated that the pact was yet to be discovered (Bernstein 2015). The American concerns expressed in the assessment by an individual may not be far from the actual given the timing of the pact. But more important is the question of some formalization of state practice of cyber alliances and collective security in case of cyber attacks. The nature of the pact is such that it co-opts much of cyber criminal and non criminal activities within a framework of cyber war. It allows states to play primary role in ensuring that nothing untoward happens to a friendly state. Such an assurance is implicitly contingent on tight control of cyberspace by the government because without such control, no state can assure an ally that nothing untoward would happen from its network. In this way, Russia-China cyber pact is a strong statement on the state regulated and controlled cyberspace. This is also the reason why this pact has been seen as Russian attempt to put an alternative model of cyberspace governance with the support of China. James Lewis, the Senior Fellow at the Centre for Strategic and International Studies, has said in the context of this cyber pact: “Russians have tried to shape how the Chinese think about these issues”. He said that the “Russians made the announcement to jerk the Americans” Another scholar Richard Bejtlich has opined that the pact may be to share technologies that improve surveillance and automate censorship. He however adds that the signing of the pact does not mean that the two are really going to “share serious tricks of the trade”(Peters 2015).

The commonalities are however are weighty. Before coming to clear terms of the pact, the Russian-Chinese interagency consultation between two countries revealed that both had common interests. Both wanted to act against the use of information technology for the use of interfering in internal affairs of a country, in undermining the sovereignty or political, economic or social stability of a country, in disturbing the peace, as propaganda for terrorism, extremism or separatism, to incite inter-ethnic or inter-religious hate or for the use of criminal or terrorist goals. The two are also strongly in favour of ‘internationalization of control’ of Internet which would weaken the hold of United States on Internet (Chernenko, et al 2014). It is these points of common interests that were put in the interagency consultation document. Out of these commonalities, the two stand out for being the causes that have pit Russia and China against US. They are issues of sovereign control over cyberspace and the internationalization of control of Internet. Both are related but are not one and the same thing.

4.2.2.4 Internationalisation of Control

Russia has been vocal on the issue of internationalization of control of Internet. In this regard, the control of ICANN () is the top most concern In order to understand the concerns of countries like Russia and China, ICANN’s role, structure and control are important points. The diagram below gives a depiction of it.

Figure 4.1: Functions of ICANN


ICANN
ICANN co-ordinates how IP addresses are distributed to avoid repetition or clashes. It is also central repository of IP addresses
Domain names are sold by no. of registrars. ICANN draws up contracts with registry and runs accreditation system for them
Operators of root servers are autonomous but work with ICANN to ensure that the system stays upto date with advances and changes
IP Addresses
Domain Name System (DNS)
Root Servers

i. *Domain Name System*: It is a system for Internet to make it accessible to people. It is millions of computers that make up the whole Internet. Computers would find it difficult to find one another without a domain name system. Computers do it with a series of number of each computer (called IP address) with each number correlated to different device. Since remembering numbers is difficult, so DNS uses series of letters and then links a precise series of letters (which is the domain name) with a precise series of numbers. A domain name does not remain tied to a computer because link between a particular domain name and particular IP address can be changed quickly and recognized by the entire Internet. A domain name consists of two parts: part before the dot and part after the dot. The part to the right of the dot which is usually ‘com’, ‘net’, ‘org’ and so on, is called top-level domain (TLD). One company (called a registry) is incharge of all domains ending with that particular TLD and has access to a list of all domains directly under that domain. It also has access to all IP addresses associated with those domain names. The part of the domain before the dot is the name that one registers. It is this part which is used to provide online systems such as websites, e-mail, etc. These names are sold by a number of companies or registrars. These registrars are free to charge any amount they wish. But usually entities or persons pay a set per domain fee to the particular registry under whose name the domain is being registered. ICANN enters into contract with these registrars and runs accreditation system for them

ii. ICANN and IP addresses: The role played by ICANN with regard to IP addresses is similar to that in domain name system. It ensures that there is just one IP address for one. This is done to avoid clashes and delay and confusion in movement of traffic. ICANN does not run the system of IP addresses but limits itself to the role of co-ordination. ICANN is also the central repository for al IP addresses. It distributes ranges to the various regional registries who in turn distribute to network providers.

iii. Root Servers: Root servers are the servers that store a copy of the same file which acts as the main index to the Internet’s address books. It lists an address for each top level domain where that registry’s own address book can be found. In practice, the root servers are more like storehouse of addresses which are consulted infrequently because once computers on the network know the address of the particular top-level domain they retain it checking back only occasionally to make sure the address has not changed. It however smoothens the functioning of the internet. The operators of the root servers are autonomous but work with one another and with ICANN to remain up-to-date. The root servers are very basic part of how internet operates. The domain name system was made because it is easier for humans to remember names than numbers but computers remember the numbers. So a system is required that can translate names to numbers. Computers help in translating that but the initiation of translation requires the number given to a computer. So, the initial number that DNS software needs to know are referred to as DNS root servers. Root servers are therefore the point of initiation. So for instance, if one types www.beagle.com, the computer would read it from right to left in parts. This means that it would be read like dot com beagle www dot. The first dot indicates the root servers. The DNS servers should know the IP address of them because they are the starting point. There are 13 IP addresses of the dot servers (Pillai 2013).

The root name servers publish the root zone file to other DNS servers and clients on the Internet. The root zone file provides description about the location of authorised servers for the DNS top-level-domain names. So, for instance, it tells which servers are authorized for names like org, net, au, etc. There root servers are operated by root servers operators. Till 2007, there were twelve organizations that were providing root server services at 13 IP addresses. The thing to be noted is that there are twelve operators but the list below consists of 13 names. These 13 are the IP addresses. So, Veri Sign has been provided two IP addresses. The capital letters indicate a particular server machine. These days, each letter identifies a single IPv4 addresses[22] at which service is provided (Karrenberg 2008).

1. A-Veri Sign Global Registry Services
2. B-University of Southern California-Information Sciences Institute
3. C-Cogent Communications
4. D-University of Maryland
5. E-NASA Ames Research Center
6. F-Internet Systems Consortium, Inc.
7. G-U.S. DOD Network Information Center
8. H-U.S. Army Research Lab
9. I-Autonomical/NORDUnet
10. J-Veri Sign Global Registry Services
11. K-RIPE NCC
12. L-ICANN

[22] IPv4 stands for Internet Protocol version 4. Internet Protocol is like postal system which provides a format in which packets of information is to be delivered. It identifies the device which is to delivered information. Version 4 allows only 4 billion addresses. Since, the number of devices have increased, the number of addresses will run out. So, IPv6 has been introduced.

13. M-WIDE Project

These root server operators are located in USA. It is for this reason that some countries complain that US has got enough edge over others because the root server operators are located in US, making them subject to law of that country.

iv. Organisational Structure of ICANN

The body is actually made of different groups and has a composite nature. Every group represents some interest and play role in decision making of the body. The supporting organizations are:

1. Organisations dealing with IP addresses
2. Organisations dealing with domain names
3. Managers of country code top level domain names

Apart from above, there are four advisory committees which play advisory role and make recommendations. They represent interests of the following:

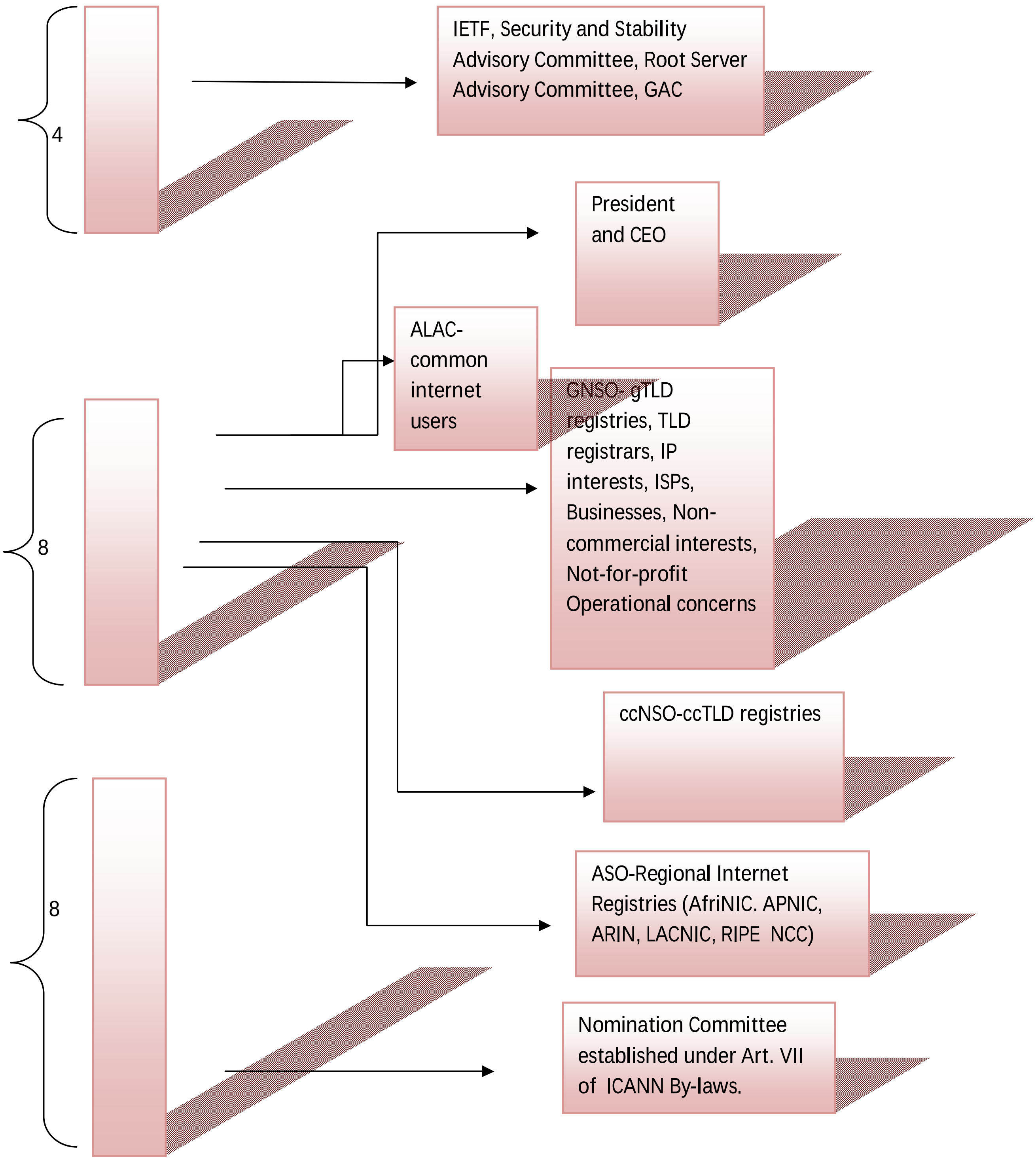
1. Governments and international treaty organizations
2. Root server operators
3. Organisations dealing with internet security
4. Average internet users

The final decisions of ICANN are made by a Board of Directors. This board consists of 20 members, out of which 16 (8+7+President) are with voting rights and remaining four are non voting members. Majority of the voting members (that is, eight) are chosen by a Nominating Committee and remainder are nominated from supporting organizations. Nominating members have to integrate the interests of various types. The remaining seven voting members are chosen by other interests. Therefore, following are the other important players in the organizational chart of the Board of ICANN and its composition:

1. Address Supporting Organisation (ASO): These are regional Internet registries like AfriNIC, APNIC, ARIN, LACNIC, and RIPE NCC.
2. At-Large Advisory Committee and At-Large Community (ALAC): These represent the interests of common users of Internet.

3. Country Code Names Supporting Organisations (ccNSO): These consist of country code top level domain name registries like .us, .uk, .au, .be, .nl, etc.
4. Governmental Advisory Committee (GAC): It plays an advisory role and allows several countries and non-state actors like Multinational companies to play a role in ICANN. The membership consists of national governments and economies recognized in international for a. The observer members are usually the multinational governmental and treaty organizations and public authorities that have interest in internet governance such as International Telecommunications Union (ITU) and World Intellectual Property Organisation (WIPO)
5. Generic Names Supporting Organisation (GNSO): The GNSO is a body that represents commercial and non-commercial interests like registries and registrar stakeholder groups.
6. Internet Engineering Task Force (IETF): This is body whose membership is open to all. It looks at the engineering aspects of the Internet. The IETF website: "The IETF's mission is to make the Internet work better, but it is the Internet Engineering Task Force, so this means: make the Internet work better from an engineering point of view. We try to avoid policy and business questions, as much as possible"
7. Root Server Advisory Committee (RSSAC): This committee advises ICANN community and it's Board on the matters of operation, administration, security and integrity of root server system. It has representatives from world's twelve root server operators and from organizations that do the maintenance of the root zone. The latter types of members of the committee are non-voting members.
8. Security and Stability Advisory Committee (SSAC): This committee advises ICANN and the Board on matters of security and integrity of the Internet's naming and address allocation systems. These security matters are related to the correct and reliable operation of root name system, address allocation and internet number assignment, registries and registrar services.

Figure: 4.2 Board of ICANN


4
IETF, Security and Stability Advisory Committee, Root Server Advisory Committee, GAC
President and CEO
ALAC- common internet users
GNSO- gTLD registries, TLD registrars, IP interests, ISPs, Businesses, Non-commercial interests, Not-for-profit Operational concerns
8
ccNSO-ccTLD registries
ASO-Regional Internet Registries (AfriNIC. APNIC, ARIN, LACNIC, RIPE NCC)
8
Nomination Committee established under Art. VII of ICANN By-laws.

The arrows in the Figure 4.2 indicate the bodies or constituents that send the representatives to the board of ICANN. For instance, the bottom bar on the left with the curly bracket and number 8 indicates the eight members of the Board that are nominated by the Nominating Committee. The arrow indicates the Nominating Committee (on the right side, bottom most box). Similarly, the next bar on the left with the number 7 indicates the seven members that are sourced from diverse interests that are indicated with the arrows and boxes. These eight plus eight members constitute the total sixteen members with the voting members. This includes the President who is the ex-officio voting member of the Board. The top most bar on the left with the number four indicates the remaining four members out of total 20 that don’t have voting rights. These represent the interests on the boxes with arrows on the right. So, the board gives representation to diverse state and non-state actors. But till 2014, it shared special relationship with United States for two reasons. Firstly, ICANN is incorporated under the law of the state of California in USA. This implies that the body is subject to US law and can be called to account by the judicial system of the country (www.icann.org). Secondly, since 1988, ICANN has been in contract with US Department of Commerce which gives power of oversight or stewardship to the department. This contract is going to expire in 2015. The Obama administration decided in 2014 that this contract would not be renewed and overturned the oversight capacity to a multi-stakeholder mechanism proposed by ICANN. FadiChehade, the President and CEO of ICANN dispelled the fears that Russia and China would now seize and control the Internet. He said: “Everyone is focused on these three, four countries..but in between we have 150 other countries that value the same values we do. Our commitment to the multistakeholder is not so much for the few who do not believe in it, it should be to the great middle mass that would like to see us stand by it and they will stand with us.” Assistant Secretary of Commerce Lawrence Stricking also said: “No one has yet to explain to me the mechanism by which any of these individual governments could somehow seize control of the Internet as a whole” Chehade referred to the power of the multi-stakeholder model to stop any kind of seizure attempt (Selyukh 2014).

Russia's stance has often questioned the American domination of the ICANN. It is apparently not satisfied with the multi-stakeholder model has been operated. The representation of diverse state and non-state actors does not do enough to mitigate Russia's doubts. The country has several interests which the status quo in ICANN does not fulfill. It wants greater control over the distribution system that connects domain names in Russia's country code top-level-domains (ccTLDs) like .ru to the domain name system of the global internet which is the basis of the Latin alphabet web addresses instead of numbers of the IP addresses. So, that would anable web users to visit www.runet.org instead of some easily forgettable long number based IP address. Secondly, Moscow wants to play greater role in ICANN but the overwhelming presence of USA even in a multi-stakeholder means that such a thing is possible if the latter cedes away some control. According to ICANN President, Chehade, the greater involvement of Russia in web domain operations would impart only some capacity to disrupt the functioning of RuNet but would not mean total surrender of control of Internet to Russia. In 2014, ICANN was reported to be unwilling to surrender control of older and popular .ru domain without broad agreement Russia among Russia's Internet society and human rights authorities. There is a fear factor behind Russia's take on the issue of ICANN's way of controlling Internet operation. Russia actually fears that in the event of a war or conflict, the rival countries may be successful in shutting Russia from the global internet. It is for this reason only that Russian Presidential office was considering to install 'kill switch'. A kill switch would make it possible to sever Russia's access to the global Internet. This fear increased when it was revealed by Edward Snowden NSA had accidentally caused internet outage in Syria (Rothrock 2014). The outage took place when the hacker team in NSA tried to gain access to the mass usage of the internet but a glitch happened and Syria went completely offline. Russia wants to take enough precaution against this kind of situation. So, the basis of the discomfiture with the status quo of ICANN is the sovereignty question. It feels that the representation of diverse interests in ICANN with an upper hand of the interests of the non-state entities do not give enough leeway to protect state actors from defending their information sphere from any kind of threats.

4.2.2.5 Sovereignty Issue in Internationalization of Control

Russia has emphasized the point in nearly every international forum that cyberspace now needs to be governed in a manner that allows state actors to have control over the sovereign information space. In this context, Russia, China, Tajikistan and Uzbekistan made a proposal titled International Code of Conduct for Information Security. The document no.A/66/359, dated September 14, 2011 titled 'Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General' (4-5), proposes eleven points to drive the point that new code of conduct is necessary to protect the sovereignty of state actors. The eleven points say that each state voluntarily subscribe to the following pledges:

1. "To comply with the UN Charter and universally recognized norms governing international relations that enshrine respect for the *sovereignty*, *territorial integrity* and *political independence* of all states, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries.
2. Not to use information and communication technologies, including networks, to carry out hostile activities or acts of *aggression*, pose threats to international peace and security or *proliferate information weapons* or related technologies.
3. To cooperate in combating criminal and terrorist activities that use information and communication technologies, including networks, and in curbing the dissemination of information that incites *terrorism, secessionism, extremism* or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment.
4. To endeavour to ensure the supply chain security of information and communications technology products and services, in order to prevent other states from using their resources, critical infrastructure, core technologies and other advantages to undermine the right of the countries that have accepted the code of conduct, to gain *independent control* of information and communications technologies or to threaten the political, economic and social security of other countries.

5. To reaffirm all rights and responsibilities of states to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from *threats, disturbance, attack and sabotage*.
6. To fully respect rights and freedom in information space, including rights and freedom to search for, acquire and disseminate information on the premise of complying with relevant *national laws and regulations*.
7. To promote the establishment of a *multilateral, transparent and democratic international Internet management system* to ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet.
8. To lead all elements of society, including its transformation and communication partnerships with the private sector, to understand their roles and responsibilities with regard to information security, in order to facilitate the creation of a *culture of information security* and the protection of critical information infrastructures.
9. To assist developing countries in their efforts to enhance capacity- building on information security and to close the digital divide.
10. To bolster bilateral, regional and international cooperation, *promote the important role of the UN in formulating international norms, peaceful settlements of international disputes and improvements in international cooperation in the field of information security*, and enhance coordination among relevant international organizations.
11. To settle any dispute resulting from the application of the code through peaceful means and to *refrain from the threat or use of force*."

Some words and portions in the above eleven points have been italicized. The italicized words indicate the points that the letter has sought to emphasize. In the first point, 'sovereignty, 'political independence' and 'territorial integrity' are the key terms which reflect the aims of the countries that have made the proposal. The common perception has been that cyberspace has been dismantling the old norms of sovereignty, political independence and territorial integrity because the free flow of information facilitates a de-territorialisation process. So, the four countries have sought to reiterate the importance and relevance of these norms. Their mention in the first point also introduces the framework within which they propose to see the information space. The second point has words 'aggression' and ‘proliferate information weapons’ which show that there is a need to see that modern means of attacks are no more different from other war weapons that have proliferated and information space is also the place of aggression. The proposal wants to take cognizance of this. In the third point, the words ‘terrorism’, ‘secessionism’ and ‘extremism’ have been put to take into account the recent rise in use of cyberspace to propagate ideas of terrorism and extremism. Russia, China, Tajikistan and Uzbekistan have also been afflicted by at least one of these three problems. So, the move to include this point is reflective of protection of their security interests. In the fourth point, the term ‘independent control’ shows that the four countries want to change the way cyberspace has been dealt with and want countries to have enough leeway to control it. The fifth point talks about ‘threat’, ‘disturbance’ and ‘sabotage’ in context of information and critical infrastructure. In recent times, cyber technologies have been used to inflict damage on the infrastructure. This point has been inserted to bring out the need to see the potential of information technologies to wage new wars in which physical infrastructure and information networks can be hit effortlessly.

In point six, there is mention of complying with ‘national laws’ and ‘regulations’ which indicate that importance that four members want to give to introduce more laws and regulations for the information space. This has come after use of information space by non-state actors to foment protests. Russia and China have been apprehensive about what these protests can do to the political stability due to absence of any law and regulation for information space. So, the presence of this point is consistent with the perspective of Russia and China on the need to have compliance with national laws. This also indicates that the proposal wants countries to see the information space as a domestic sphere that should be subject to laws which are used to control other domestic areas. The seventh point talks about establishment of ‘multilateral’, ‘transparent’, ‘democratic’ and ‘international’ Internet management system is reflective of the type of the system that the four countries visualize and is an attempt to change the status quo in which ICANN and USA are perceived to be major players. This also indicates that four countries do not view the current system and structure as multilateral, transparent and democratic. These three terms are not likely to be dismissed by any state actor as the terms seek involvement of more actors. So, the point is a measure to invite even players who are less inclined to support state controlled cyberspace, to come forward and support the proposed system. In the eighth point, there is mention of need to have a ‘culture of information security’. The word culture indicates a broad system which subsumes many practices. So, the proposal seeks to bring a very broad system in which countries seize the opportunity to bring within the purview of security activities in information space. The tenth point talks about the ‘role of UN in formulating international norms’, ‘peaceful settlement of disputes’ and ‘international cooperation in information security’. This is the point that talks about the need to avoid shying away from accepting the reality of cyber wars and disputes arising from them. The number of cyber incidents has increased but countries have rarely come out openly accusing a state actor. This may be due to the absence of a mechanism to resolve the disputes and conflicts. The tenth point of the proposal seeks to address that lacuna in the existing system. This also implies that proposal wants states to accept the reality of warfare in modern realm of information, although the point does not explicitly mention the word warfare. The last point carries forward the same by talking about the need to refrain from threat or use of force. This sounds similar to many measures enshrined in international covenants that seek to discourage outbreak of war. Therefore, the proposal put forward by four countries is both traditional and futuristic. It is traditional because it reaffirms the place of norm of sovereignty and role of state actors. On the other hand, it is also futuristic because it takes into account the potential situations that may arise due to increasing tendency to use information space for warfare. In both cases, it is the sovereignty and role of state that are emphasized. So, the cyberspace governance that the proposal visualizes is state led and is within the framework of security. In line with this proposal, Russia put forward its own draft Convention on International Information Security in 2011 and published it in the website of Russian Embassy in London. This concept of convention is not only Russian take on cyberspace governance but is also a response to the European Convention on Cyber Crime which came into existence in 2001. Both are competing versions of cyberspace governance and have differing points of emphasis. A comparison between the two is given below to bring out similarities and differences.

Table 4.1: Comparison between European Convention on Cyber Crime and Russia's Convention on International Information Security

European Convention on Cyber Crime	**Convention on International Information Security**
The Preamble of the Convention mentions the important need to pursue 'a common criminal policy' for 'protecting society' against cyber crimes through appropriate legislation and international co-operation (See Appendix1)	The Preamble's key things as 'threats connected with the possible uses of ICT technologies and means for purposes not compatible with measures to ensure international security and stability", both "military and civilian spheres". It talks about creating legal and organizational basis for cooperation between states in the sphere of international information security (See Appendix 2)
Preamble recognizes the important role of private industry in combating cyber crimes and mentions the need for cooperation between private sector and state actors to protect legitimate interests in use and development of information technologies	Preamble also talks about the role of private sector. It talks about the "necessity of cooperation between governments and private businesses in fight against illegal activity in the information space and the necessity of protecting the legal interests of parties involved in use and development of ICT" (See Appendix 2)
There are 48 articles out which 35 articles deal with various aspects of cyber crimes like nature, investigation, prosecution and jurisdiction.	There are 23 articles out of which 13 articles are regarding information security issues like information security like information warfare, military conflict in information space, use of the information space and technologies by terrorists, international cooperation and confidence building measures in the military

	use of information space. Only article 10 and article 11 are actually about cyber crimes. These also are subsumed under the bigger category of “illegal activity in information space”
It is basically a convention to tackle cyber crimes of various types	It is a draft document for establishing a norm of information security with cyber crimes subsumed under it.
According to Article 22 , clause1, dealing with jurisdiction, each party shall adopt legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of Convention, when the offence is committed: a. in its territory; or b. on board a ship flying the flag of that Party; or c. on board an aircraft registered under the laws of that Party; or d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. (See Appendix 1)	The whole document is having the word jurisdiction at several places but the clause similar to Article 22 clause 1 of European Convention is there in Article 11, clause 8 which says that States Parties shall: “take legislative or other steps to establish its jurisdiction over any criminalized and socially dangerous action in the information in the information space perpetrated in the territory of the State, on board a vessel flying the flag of that, and on board a plane or any other aircraft registered under the laws of that State. (See Appendix 2)
Under Article 22 of the Convention calls for consultation	Under Article 11 of this Convention, interested parties are to hold

between parties in case more than one party claims jurisdiction over an alleged offence established in accordance with the Convention, with a view to determine the most appropriate jurisdiction for prosecution.	consultations to decide on the most suitable jurisdiction for prosecution if the jurisdiction over an alleged offence is claimed by more than one State party.
The convention gives important role to state actors but is not about reaffirming the sovereignty of state actors	The convention strengthens the sovereign right of state actors over information space. The word sovereignty is mentioned in many places.
The convention is mostly about cyber crimes.	The convention is about increasing use of information technology for warfare involving both state and non-state actors. So, it is rich in issues that have to do peace, security and warfare.

Source: Appendix 1 and 2.

The Table 4.1 has brought out the similarities and differences between the two conventions. While similarities are due to the fact that over the course of time certain activities like cyber crimes have become usual, the differences are due to fast changing scene in cyberspace. The European Convention was formed when cyber crimes were new and state actors had not started getting involved in cyber warfare. Cyber warfare had not become the buzz word. So, the convention focuses on cyber crimes that were becoming common at the turn of the millennium. The jurisdiction issues however arise in matters of crimes and prosecution. Therefore, European Convention extensively discusses the ways to deal with them. The proposed Russian Convention borrows some of those jurisdiction provisions. But, it has gone far beyond the European Convention in terms of the main focus.

Russia's proposed concept is much more contemporary because it takes full account of the two things. Firstly, it discusses information security, information warfare, peace and security, military conflicts in information space and possible conflicts that may arise due to them. Since, states are more openly accusing each other of waging cyber war, the document sits well with the current needs. Secondly, in matters of cyberspace governance, the role of state actors has often been called into question due to the nature of cyberspace. This Russian document gives a supreme place to the state actors and the sovereignty norm. Russia's proposal is therefore a reflection of the evolution in the cyberspace and the practices of state actors in the information space.

In line with the thoughts about what state actors ought to do, Russia took the opportunity to begin cyber security dialogue. The two countries then finally created a working group under the auspices of Bilateral Presidential Commission for emerging ICT threats. They also took some measures in the nature of confidence building measures. The two decided to arrange for sharing of threat indicators between the Computer Emergency Readiness Team of two countries. The two are supposed to exchange technical information about malware or malicious indicators that appear to originate from each other's territory and to aid in proactive mitigation of threats. The second confidence building measure included authorization of a direct and secure voice communications line between the U.S. Cyber security Coordinator and the Russian Deputy Secretary of the Security Council. It is kind of hotline that will be used to manage crisis situation. The two countries also decided to use the longstanding Nuclear Risk Reduction Center (NRRC) links that was established in 1987 between USA and Soviet Union to build confidence through information exchange with the help of round-the-clock staff at Department of State in Washington D.C., and Ministry of defense in Moscow. This new use would allow both to make quick and reliable inquiries from each other's competent authorities to reduce possibility of misperception and escalation from ICT security incidents (White House Press Secretary, June 17, 2013). Therefore, Russia has taken proactive measures to strengthen the role of state actors in driving the cyberspace governance.

4.2.3 A Legal Approach to Cyberspace

This approach is common in the domestic sphere of a country because the latter can be modified and controlled through laws and regulatory measures. Apart from the surveillance related regulatory measures, Russia has taken number of measures that fall under this category. These have been taken to deal with view to curb crimes, social problems and to fulfill business interests. In June 2013, Russia took one of the toughest measures to tackle online piracy. The lawmakers fast tracked a bill that allows copyright holders to complain directly to courts if the material infringing copyrights laws was found in a website, without contacting the website. If the rights holder wins the case and the content in question still remains in the site, the website's IP address will be blacklisted by Russian ISPs. The web companies were worried about the law because blocking IP address would mean many other sites would also be engulfed in the blacklist. Russia's Google and Yandex, the search engines in Russian internet market were unhappy about the move to bring such legislation and some amendments were proposed by tech giants that could make the legislation less punitive. But the lawmakers went ahead with fast tracking and had both the readings of the bill in one day. Yandex reacted to the action by saying: "This approach is technically illiterate and endangers the very existence of search engines, and any other Internet resources. This version of the bill is directed against the logic of the functioning of the Internet and will hit everyone-not just internet users and website owners, but also rights holders. It's like forever closing the highway, on which there was only one accident."(Andy 2013). Along with this, another bill was rushed through and signed into law quickly by President Putin. This second law is about a list of websites to be blacklisted. Under this law, any website can be blacklisted whose content is deemed to be unsuitable or harmful. Both these laws were compared to Stop Online Piracy Act (SOPA) of United States which was sought to be introduced in the country was not because of strong opposition from every quarter.

In Russia, the anti-piracy bills were introduced to protect interests of creative and entertainment industry that included movies and music. But other aims like curbing the social problem of suicides was also a factor in rushing through the bill. Alexei Pimanov who is a host for Russia's most popular TV channel claimed that he had co-authored the bill with the aim to improve country's ailing film industry. Under the newly introduced law, an educational cartoon was banned. The cartoon popularly called ‘Dumb Ways to Die’ was designed to promote safety awareness about the dangers of public transport. The cartoon was in the genre of black humour and had won critical acclaim at international ad festivals. The cartoon went viral in 2012 when its popularity soared. But Russian authorities banned it under the new legislation because they felt that the cartoon promoted suicide. Under the same law, the Russian Wikipedia page about cannabis was removed because it was found to be in the nature of promotion of cannabis (Richet 2013). The law is called the ‘Federal Law No. 187-FZ of July 2, 2013 on Amending Certain Legislative Acts of the Russian Federation on Issues of Protecting Intellectual Rights in Information Telecommunication Networks. Under Article 3 of the law, the procedure for restricting access to information disseminated in breach of exclusive rights to motion pictures and television films has been dealt with. It says:

1. “If films, for instance cinema films or television films, or the information required for getting them through the use of information telecommunication networks have been discovered in information-telecommunication networks, for instance in the network “Internet” which are disseminated without the permission of the right holder or without another legal ground, the right holder is entitled to file an application-under a court’s judgment that has become final-with the federal executive governmental body in charge of control and supervision in the field of mass media, mass communications, information technologies and telecom for measures to be taken for restricting access to the information resources which distribute such films or information. The form of said application shall be endorsed by the federal executive governmental body in charge of control and supervision in the field of mass media, mass communication, information technologies and telecom.”

   After the above measure in Article 3 of the law, the following measures have been recommended:

2. On the basis of the court’s judgement, the federal executive government body that is in charge of control and supervision in the field of mass media, mass communications, information technologies and telecom shall do the following within three working days:

(1) identify the hosting provider or the other person ensuring the placement of information resource in an information-telecommunication network which provides services to the owner of a website in the network Internet containing the

information containing the content or the information required for getting them through use of ICT networks without permission of the right-holder or without any another legal ground.

(2) send a notice in electronic form in Russian and English to the hosting provider or other person mentioned in previous point about the breach of rights of holders allowing them to identify the website that has been used to information containing the motion pictures or the information required for getting them through use of ICT, and also the pages of website that allow such information, for measures to be taken to delete such information.

(3) fix the date and time of the dispatch of the notice to the hosting provider or other person mentioned in part 1 of this part.

After this following steps (in continuation of previous mentioned part) are suggested:

3. Within one working day, the hosting provider or the person mentioned in part 2 (1) shall inform accordingly the owner of the information resource to whom they provide services and notify him about illegal deletion of the information or restricting access thereto.
4. Within one working day after receiving such notice, the owner of the information resource shall delete the information concerned. In the event of refusal or omission by the owner of the information resource, the hosting provider or the person mentioned in part 2(1), shall restrict access to the relevant information resource within three working days after the time when the notice is received.
5. If the measures mentioned in (3) and (4) are not taken, the domain name of the Internet website, its web address, the page indices of the website on the Internet that allow identification of information containing motion pictures content or the information required for getting them through use of ICT, shall be sent to the communication operators for restricting access to that information resource.
6. The federal authority mentioned in part (2) shall, within three working days after receiving court’s judgement on restriction on access to an information resource, notify the hosting provider or the person in part 2 (1) and the communication operators of the measures for restricting access to the information resource concerned.

7. Within 24 hours after receiving via the information about the information resource containing motion picture material or other information required for getting them without permission of rights-holder or without any legal ground, the communication operator shall restrict access to such information resource.
8. The procedure for operating the cooperation information system shall be established by the federal executive governmental body which is in charge of control and supervision in the field of mass media, mass communications, information technologies and telecom.

The authority mentioned in point 8 is actually the Roskomnadzor, the body that deals with the area mentioned there. Also, the procedure mentioned in Article 3 from the identification to the final restriction will take only few days if each step is strictly followed. The procedure mentioned above with all the steps has to follow filing of application for preliminary protection of rights for the content concerned with Moscow City Court. This is part of the Article 2 of the new law. The law was perceived to be mechanism to be harmful to the interests of the end users and also sites that contain such material. Therefore, it attracted ire of many sites and major search engines.

In protest against the law, around 1700 websites went dark. The Russian branch of the Pirate Party launched a Black August campaign (Smolaks 2013). An online petition against the anti-piracy laws also received 100,000 signatures (the number of signatures necessary to send the document for government discussion. Under the Russian Presidential decree, public initiatives that receive support of at least 100,000 signatures of citizens can be sent to the government for discussion). The authors of the document urged the government to suspend the law which they believed lacked clarity and did not observe the presumption of innocence and allowed violations on the part of copyright holders (RT 2013). But the government in 2014 made the earlier anti-piracy law even stricter. According to the amendments, areas for website blocking have been expanded. Earlier, the law introduced in 2013 was limited to video production but the 2014 amendments approved by President included all kinds of copyrighted content such as books, music and software. Only photographs were left. In addition to this, websites guilty of more than one copyright violation will be permanently blocked in the country and once blocked, the sites cannot be unblocked.

Russia also introduced a law for data protection in July 2014 according to which personal data operators are required to store and process any personal data of Russian individuals within databases located in Russia. The penalty for violation of this is the blocking of websites involving unlawful handling of Russian personal data. The law is called Federal Law N 242 FZ. The provision for Register of Offenders is given in Article 1 of the law itself. It says that:

1. "In order to limit access to information in the Internet which is in violation of the law of Russian Federation in field of personal data, an automated information system called Register violators will be there"
2. "The register of offenders includes:

1.) domain names and or signs of pages of sites in the Internet, containing information that is in violation of the legislation of the Russian Federation in the field of personal data;

2.) the network addresses that identify network sites Internet, containing information processed in violation of the laws of the Russian Federation in the field of personal data;

3.) an indication of the entering into force of the act;

4.) information on elimination of violations under the legislation of Russian Federation in the field of personal data;

5.) the date of the direction of operators on the information resource to restrict access to this resource"

The part 7 of the law explains the procedure that would be followed in dealing with the offending site. It says:

7."Within three working days of receipt of an enforceable court decision, the federal executive authority exercising functions of control and supervision in the sphere of mass media, mass communications, information technology and communications, on the basis of the said decision of the court shall:

1) determine the hosting provider or other person providing the information processing in information-telecommunication network, including Internet, in violation of the laws of the Russian Federation in the field of personal data;

2) direct the hosting provider or other specified in part 1 in electronic form a notice in English and Russian languages on the violation of the legislation of the Russian Federation in the field of personal data with information about which entered into

force with court act, domain name and network address allowing identification of the site in the Internet, where information processing is carried out in violation of the law of the Russian Federation in the field of personal data referred to in the judgement.

3) fix the date and time of notification or any other hosting provider referred to in the paragraph 1 of this of the person in the register of offenders.”

The part 8, 9 and 10 of Federal Law N 242 FZ of Article 1 deal with subsequent process and are as follows:

1. “within one business day of receipt of the notification referred to in paragraph 2 through 7 of this Article, the hosting provider, or a person otherwise referred to in paragraph 1 of part 7 of this article, is required to inform the owner of the information resource they serve and to notify him of the need to take immediate action to eliminate violations of the law of the Russian Federation in the field of personal data referred to in notification or take measures to restrict access to the information processed in violation of the law of the Russian Federation in the field of personal data.
2. Within a business day of receipt by the hosting provider or a person specified in paragraph 1 of the part 7 of this Article, of the notice about the need to eliminate violations of the law of the Russian Federation of personal data, the owner of the information resource is obliged to take corrective measures specified in the notice of the violation. In case of refusal or omission of the owner of an information resource, the hosting provider or the other person referred to in paragraph 1 of part 7 of this article is required to limit access to the appropriate information. It should not be later than three working days of receipt of the notification referred to in paragraph 2 of part 7 of this Article.
3. In the event of failure or other hosting provider or the person referred to in paragraph 1 of part 7 of this Article and or the owner of an information resource to take action, the domain name of the site in a network Internet, its network addresses, index pages in the network of Internet that enable identification of the information processed in violations of laws of Russian Federation in the field of personal data as well as other information about this site shall be sent by an automated information system by telecom operators to limit access to this information resource.”

In addition to the above parts and their sub parts, the Article 2 of the new law mentions the requirement of having database within the territory of Russian Federation. It says:

“When collecting personal data, including through information technology network Internet, the operator is obliged to provide a record, systematization, accumulation, storage, clarification, extraction of the personal data of citizens of the Russian Federation with the use of databases in the territory of the Russian Federation (Federal Law N 242 FZ, Article 2).”

A database is a collection of information organized in such a way that a computer program can easily select desired pieces of data. In a traditional database, data are organized by fileds, records and files. Field is a single piece of information, record is one set of field and file is a collection of records. Another type of database system is the hypertext system which was invented by Ted Nelson in which objects (that is text, pictures, music, programs etc) can be linked to each other. So, when an object is selected, one can see all the linked objects. This system facilitates not just browsing but also organization of database. A database management system is a collection of programs that stores, modifies and extracts information from a database. Database server is a system of powerful computers that manage network resources and manage database queries. A query is a request for information. This means that servers are key things to the database management. Russian Law requires the servers to be located in the Russian territory. This is to facilitate better control the data of citizens and tighten the grip over the information sphere of the country. It is akin to strengthening the sovereignty of the country in practice of cyberspace governance. Since, it comes in the wake of NSA snooping revelations by Edward Snowden, they are also about preventing other countries from accessing data of the citizens. According to Malloy and Arievich (2015), the said law is likely to place burden on a number of international businesses that are doing business online like travel companies. This is because many operations require routine processing of data of individuals from all countries without having a presence in Russian. The requirement of law would demand the businesses to distinguish the data related to Russian individuals and store them in a server in Russia. This implies that in order to facilitate their business, they would require a Russian presence. This also reflects a security concern on the part of Russian lawmakers. However, it has been found that those who support stringent laws for dealing with online activities have other reasons which have been thrown at the opponents of the new changes. For instance, in 2012, Russian Parliament unanimously adopted a bill that called for a federal website ‘no’ list of site owners and internet operators to shut down. In the discourse on that bill, the supporters of the bill argued that the ‘no’ list was designed to crack down on child pornography as well as sites that promoted drug use and teen suicide. Those opposing the bill thought that the term ‘bad content’ was too vague and could lead to blacklisting of just any site. The Parliament took cognizance of that vague language and replaced it with terms child pornography, promotion of drugs or suicide. Still, the bill was not received well by internet giants of the country. The chief editor of Yandex wrote at the time: “The need to fight child pornography and illegal content are as important for civil society as the support of constitutional principles like freedom of speech and access to information. The proposed means provide a means for possible abuse and raise numerous questions from the side of users and representatives of internet companies.” But bill’s co-author retorted to the arguments of those opposing by terming them “paedophilia lobby” (Elder 2012). This kind of discourse is not much different from those that other parts of the world have had in the past and still do. Content filtering and blacklisting of sites are the practices that states have been found to resort for restraining circulation of content that is deemed culturally offensive or is seen as encouraging crimes. Due to this, the lawmakers have had many clashes with the interests of internet activist lobby that is fighting for freedom of expression in Internet. Since, the Russian attempt to regulate the content came soon after role of social media in fuelling Arab Spring protests, the internet activists in Russia found it a beginning to throttle the Internet.

However, the law that has been seen as the most draconian in the country is the recent law on blogging that has been introduced. According to the new amendments made in 2014 and brought into force from August 1 of the same year, the popular bloggers are required to register with the state watchdog Roskomnadzor, disclose their identity and follow the same rules that journalists are required to follow in conventional state-registered mass media. The amendments define a popular blogger as someone whose internet page attracts at least 3000 readers every day. These visitors should be uniqueand not just in the nature of page hits. Other restrictions have also been introduced. This includes the demand to verify information before publishing it and abstaining from releasing reports that contain slander, hate speech, extremist calls or other banned information (like the ones related to suicide). The bloggers are also banned from using obscene language, making heavy, drawing heavy criticism and mockery from the online crowd. In addition to these requirements, Roskomnadzor informed that law was not be affected by the physical location of the web authors because everyone writing in Russian and targeting Russian audience had to comply with the rules or else their content was bound to be blocked on the Russian territory. The fine for the individuals who violate the law is between 10,000 and 30,000 rubles. The fine is higher for popular blogs that are maintained by legal entities, amounting to 500,000 rubles. The law has been unpopular with Russian internet companies because it involves additional responsibilities and limitations. Due to this, some measures to bypass the law started soon after the law was announced. Yandex stopped publishing the statistics on blogs and LiveJournal which is the most popular blogging platform, also brought alteration in reader's statistics. State officials were unperturbed by such steps as they claimed to have their own tools for counting visitors (RT 2014). The law is not likely to be a threat to individual bloggers according to Russia's internet guru Anton Nossik, but could provide legal grounds to block popular social networks like Facebook, Twitter, LiveJournal and Google (BBC News 2014).

4.3 Conclusion

Russia has utilized the international environment to put forward its approach to global cyberspace governance. The country has entered into bilateral and multilateral pacts and agreement on cyber security with two important players in the global politics: United States and China. Through these agreements, it has not only reiterated the importance of understanding cyberspace governance through prism of peace, security and international cooperation, but has emphasized the ever more relevance of norm of sovereignty. Be it the agreement with China or the one with USA, it has sought to drive the point that state actors have a role to play. This is reflected in the terms of the agreements and arrangements that have been arrived at with USA and China. The agreement with China particularly is about putting in strong footing the place of state actors in giving a secure information space to their respective citizens. On the multilateral front, Russia has led the like-minded countries to change the status quo in global cyberspace governance. By submitting a proposal to the United Nations with the help and support of China, Tajikistan and Uzbekistan, it has sought to extend its approach to international fora and addressed the underlying need felt by many state actors to increase their role in cyberspace governance. The Russian approach is reflective of the current times which have seen ever increasing surveillance and use of ICT to control and discipline citizens. Its information security centric approach is also a symptomatic of a world that has a number of cyber wars in the last one decade.

On the domestic front, Russia has been taking a number of steps to tighten its grip over the cyberspace. This has been done by making several amendments and introducing new laws. These laws have sought to either ban ‘bad content’ or deal with increasing cases violations of intellectual property rights. The ban on ‘bad content’ is intended to deal with type of content that affects society badly (online pornography, paedophilia, suicides) or affects the political stability. The intellectual property violations in cyberspace have increased over a course of time in Russia. This has happened due to dawn of new ways to share knowledge and entertainment content. All the laws however have not been viewed in the same manner by all actors in Russia. Some giant internet companies have often found themselves at the receiving end of the new laws.

5.1 Introduction

Cyberspace continues to attract attention of governments around the world. This is because greater number of people is now connected online than twenty years ago when most social media companies had not grown. Institutions, offices, homes, and individuals are not only connected but are dependent on cyberspace. This dependency and connectivity have brought vulnerabilities. The vulnerabilities can be seen in the increasing frequency of cyber attacks. Also, cyberspace has challenged the way many operations take place in offices, the manner in which people now gather facts and express themselves. It is easier to reach wider audience now with social media. Governments cannot take its citizens for granted as greater transparency has come about with this. However, with these changes, the scope for government has also increased and state actors today are more inclined to have a mechanism to govern cyberspace. The thesis analyses this in context of Russia.

5.2 Hypotheses

There are two hypotheses with reference to which the conclusions have been arrived. The first one states that Russian position on regulating cyberspace transforms the focus of cyberspace governance from ungovernability of cyberspace to cyber control by states. The second hypothesis states that Russia's notion of regulation is informed by presence of online political activism and cyber crimes in Russia. To analyse both hypotheses, some terms have been discussed in the chapters one to four and the issues related to them. The first in this is the term cyberspace itself. While analyzing the existing literature, it has been found that the term has been used loosely and boundary between what is cyberspace and what is not has been porous. There is multitude of opinions on it, all coming from one or the other political viewpoint. That cyberspace is a result of technological evolution is a settled fact for the contribution of changes in computing technology is seen as an almost obvious fact. But it is not pure technology. There is human-machine interface at every step of cyberspace which makes it pervasive in human society and provides enough leeway for machines and humans to manipulate each other. It is in the area of this manipulation that much of the evolution of cyberspace has taken place and it is still evolving. It is important to attribute to this interactive part the role it has been playing in evolution of cyberspace because it is this which has much to offer to understand better the boundaries of what constitutes and defines cyberspace. Putting in few words a definition of a term which is still evolving is like grab water with hand. The more one tries to capture water, the more it slips out leaving nothing in the hand, a difficult undertaking.

To undertake the task of understanding what is cyberspace, the chapter one has first analysed the literature that exists, both old and a relatively recent one. The literature provides understandings each based on the perspective of the discipline or the issue at hand. The security perspective, for instance finds the militarisation as the defining feature of the domain of cyberspace while regulatory role of state is seen in state centric analyses. Since cyberspace has computing technology at the centre, there is also a view that looks at the technological aspect of the term. This poses problem for analyzing any hypothesis. The way out is found by developing a framework. That framework developed here is captured in Invention-Innovation-Practices-Spread-Entrenchment (IIPSE) cyclic process. The assumption that stands at the base of the framework is that technology evolves in a cyclic process of first getting merely invented (accidentally or purposefully), next getting innovated with its usage by society, next giving rise to practices from increased usage and spreading through trade, human interaction and getting established in the society in a way that it becomes more than just common. It becomes pervasive and widespread, making the ground for new technological breakthrough. Cyberspace too has been put in this framework to understand its domain. Beginning with invention in the computing technology which in turn took place in the churning in the defense technology that had got entrenched in that sector, the nascent Internet evolved with human usage and constant need to update it. This led to innovation in several areas of uses of connectivity of World Wide Web, spreading the new usages to an extent that they have now become practices. Some uses and practices have spread. This can be seen in the technology of social media that is a direct offshoot of spread of Internet. Internet which was invented with the initial purpose of securing American domestic military installations from nuclear attacks from Soviet Union, was ultimately innovated into something different when it spread. When it was adapted to suit different needs, it turned into World Wide Web (www). From there, the technology was further innovated to connect with each other resulting into concept of online social media. Facebook, Twitter, Instagram, Telegram, Russia’s Vknotakte, China’s Sina Weibo are all versions of social media platform. Social media has given rise to new online habits of ‘expressing online’ in which one is inclined to share views, photos, facts, news and everything that is available on the net. It has in this process been improvised further though use to become a medium of asserting oneself politically. Be it the fundamentalist expressing his or her rage against the system or the state unleashing propaganda or the terrorists using it to share graphic details of their attacks, it is tool at the hands of ‘online political creatures’ So invention through series of innovations has given rise to common practice of using social media for political ends. In a number of countries like Bangladesh, Iran, Saudi Arabia, India, Pakistan, China, Russia, USA, Germany, France, blogging has been innovated to serve the political purpose of making oneself heard in politics. A new crop of bloggers have come up who have been vocal about expressing dissent through images, songs, videos and simply jokes. Social media is therefore one of the instances where one can see the IIPSE process at work. The other is the security framework. During the nascent stage of Internet, there were not many cyber threats. This was because internet had not spread. However, once it became widespread, it got into the hands of all kinds of actors. At the hands of some non-state actors, it has been innovated into domain for committing theft of money, information, blackmail through ransomware, tool for causing economic destabilization(through Distributed Denial of Service Attacks (DDoS) attacks), and putting systems like nuclear power plants and missile systems at risk through malware. These are few among a class of cyber crimes that have emerged as a result of innovation by cyber criminals. Therefore, cyber crimes are also examples of how technology in a human-machine interface can undergo innovation and give rise to new class of cyber crime practices. The IIPSE process is at work here. This IIPSE process is important for defining cyberspace for the purpose of this work for it tries to capture what is at work in a simplified way. According to this, cyberspace is not just network of machines (mainly computers) or a total virtual space that has been understood as unreal. It is also not just social media or mere controlling systems for missiles nor are cyber crimes the totality of cyberspace.

Cyberspace as understood within IIPSE framework is an evolving systemic relationship between computing machines and humans with information as its flow. It is an interactive framework with both computers and humans exerting influence on each other. So, sometimes it appears social media has changed the way people politicize issues but seen from other perspective, people too have changed the way social media or internet has to be used. It is this definition of the term cyberspace which the first hypothesis subjects to analysis and which has been elaborated in the first chapter.

The other terms in the first hypothesis which need delineation are the terms 'regulation' and ungovernability. The term regulation includes a number of actions taken by governmental bodies in the form of laws, legislations, rules, control mechanisms to deal with situations and issues arising out of spread of cyberspace. Regulatory measures usually arise out of the need to adapt to the needs of the new scenario. Cyberspace has given rise to a large number of issues that need to be understood and adapted to. The contents of chapter 2 that deal with some of these issues have described how these issues affect the diverse fields and are in many cases the site of contestation between state and body corporate, corporate and civil liberties advocates, state and civil liberties advocates and between two different perspectives on role of Internet on knowledge dissemination. There are also different perspectives on who ultimately ought to control Internet. Out of many, chapter 2 has described issues arising from militarization of cyberspace, understanding of cyberspace as a resource and control of Internet, and Multistakeholder model VS State Regulatory model of cyberspace dichotomy.

Analysis of increasing militarization reveals that states, primarily USA are now inclined towards using cyberspace as a battle zone and consider it so. There have lately been fast developments of some cyber tools to wreck systems and conduct information theft. Military and security institutions and related bodies, important government offices and institutions, officials and websites, business bodies have faced attacks from malwares meant to disrupt the system or to snoop or to pilfer the strategic information. Innovation has an important role to understand this. A constant innovation has led to multiple cyber tools which can be made to play these roles. The response of states to this has been to further this process by bringing to the forefront the security and defense organizations to better deal with these threats and attacks. The result is a scenario in which countries do not hesitate to incorporate cyber systems in their defense and warfare. USA, China, Russia, India, Germany are known to have taken substantial measures to do so. The direct consequence of this is militarization of cyberspace and the gradual increase in the presence of state's military apparatus in cyberspace. This has resulted in front door entry of state in controlling the cyberspace which would fall under regulation of the domain by means of control through security apparatus. Surveillance in cyberspace of ordinary citizens and non-citizens is also being increasingly incorporated into the overall security policies of a number of countries. The technologies that were initially developed to conduct surveillance on a small scale now find loyal buyers in a number of countries fearing political dissidence and external security threats. It is now widespread practice among states to such an extent that most countries engage in cyber surveillance in varying degrees. From the perspective of economics, cyber security and surveillance industry directly benefits out of states' presence to control security.

The state has furthered its regulatory presence in a more nuanced way in some other sphere. This is the sphere in which state has been expected play the role of a referee or an umpire. The contestation is between two sides. One is that whatever is available in cyberspace should be left free because that is how it supposed to function and internet for the sake of principles should be left free. In this, the most contentious have been the online copyrights and the net neutrality. Technological developments have enabled people to develop means to have access to vast body of knowledge and sources of entertainment. Movies, books, other creative works can be easily downloaded for free in a number of sites and these sites have become means of spread of such body of knowledge and entertainment. Seen from the spread of ideas, cyberspace has made it possible to have easy access to things that would cost money if purchased elsewhere. But that has also led to works of art and intellect getting used without any benefit going to the owners of their owners of intellectual property rights. The interests of the intellectual property owners and the free accessibility that cyberspace has provided to wherever internet is accessible clash with each other. Those who are enabling such free access have all along said that this is how internet is and is supposed to be because right from its stage of birth, it grew spontaneously without push by governments. Curtailing such freedom would be akin to killing the true nature of Internet. But the advocates of intellectual property rights have been lobbying hard with governments to be stricter with how certain works are accessed to and used and have called free use in cyberspace a theft. The governments have taken a number of measures to deal with this new type of situation in copyrights and other IP rights. Chapter 2 has discussed in detail the case of two laws, Protection of Intellectual Property Act (PIPA) and Stop Online Piracy Act (SOPA) and how it attracted very angry and strong response from citizens, civil society members, and technology giants like Google. Some of the hacker groups like Anonymous responded by causing cyber attacks on the companies that have always advocated curbing online piracy. These attacks have been targeted at other institutions outside USA as well indicating that there is a global lobby that is totally against governments regulating this part of the cyberspace. The online copyrights issues are an indicator of innovations leading to practices that in turn call for governments to play role of a regulator. Net neutrality which means Internet Service Providers (ISPs) will not discriminate between services and websites in providing access is also a contentious issue in which governments find themselves moving to place several rules to satisfy fulfilling of a neutrality principle. Most internet based companies have found neutrality to be important because such businesses have flourished in an environment which net neutrality has provided since the spread of Internet. That Internet is a free resource which cannot be provided to people in a compartmentalized, cherry picking manner based on charges, is almost an established principle. Therefore, governments have been compelled in some countries to regulate to ensure that a principle that developed through spontaneity should remain alive. This is an instance of regulatory role of governments in favour of innovation.

The regulatory role of government has attracted maximum attention in the tussle between Multistakeholder VS State Regulatory Model of cyberspace governance. Multistakeholder approach remains fuzzy including wide ranging issues, from digital divide to copyrights, while State Regulatory approach is clearer about how it wants to see cyberspace operate. This is because proponents of regulation know that cyberspace has evolved to such an extent that either one can remain out of it at one's own peril or enter it to control it in one's favour. The innovations have led to practices among states and corporate to an extent where regulation itself becomes a kind of innovation arising out of them. Blocking access to copyright violators online, putting surveillance mechanism, blocking child pornography sites, developing cyber weapons and cyber war doctrines are some of the innovations that state has mastered to play its regulatory and controlling role.

Much of regulatory roles that governments are playing in various degrees have a direct bearing on the governance of cyberspace. The first hypothesis has used the term 'ungovernability'. There has been a dominant position that the inherent nature of cyberspace is such that it is really not governable. The governments cannot control it the way they can some other matters of governance like security, education and that any attempt to do so will infringe on some other country/countries' sovereignty. That should effectively make it some kind of global commons which cannot be subject to ownership by few states. It is true that cyberspace looks more like spontaneously developed system that is not owned by anybody, any country or body corporate. It is difficult to trace cyber crimes; currency operated in cyberspace for many transactions is the electronic currency bitcoin which is not regulated by any country and violators of an online copyright are to be found in several countries. Many non-state actors work in a global network on the basis of ideology and not for any country. Such features make cyberspace look like ungovernable. This is also fuelled by the argument that cyberspace developed in a spontaneous manner because it was not controlled by any entity. This contention falls flat in the wake of new ways governments have found to register their presence in cyberspace in their capacity as users and regulators. The militarization of cyberspace has been the battleground for supremacy among state actors and the latter have been at the forefront of it. This has left enough scope for challenging the ungovernability aspect of cyberspace and it is this which has been exploited here. The first hypothesis has mentioned Russia's position on regulating cyberspace as a causal factor that weakens its ungovernability and takes it to the opposite spectrum of control by states. The study has gathered some facts which seem to strengthen the hypothesis:

1. Russia's strong cyber surveillance system: The country's surveillance system comes under the SORM (System for Operative Investigative) series. It has been

updated thrice SORM-1, SORM-2 and SORM-3. The first part of the series was set up in 1995 that allowed Federal Security Service (FSB is its Russian acronym) to monitor telephone communications. The second part was established in 1998 that allowed monitoring of internet in addition to telecommunications. This one made it mandatory for Russian Internet Service Providers to install special device on their servers to allow FSB to track all credit card transactions, e-mail messages and web use. The device had to be installed at the expense of the ISP. Some ISPs were said to have established direct communication links with FSB. This was followed up by Ministry of Information Technology Order No. 130 which was titled 'Concerning the introduction of technical means ensuring investigative activity in phone, mobile and wireless communication and radio paging networks'. It exempted FSB from providing telecommunications and internet companies the documentation on targets of interest prior to accessing information. The latest is SORM-3. Under the new order, requirements for the new wiretapping system have been introduced. According to SORM-3, the targeted surveillance is aimed at: Single IPv4 or IPv6 address, IPv4 or IPv6 networks identified with address mask, User ID within telecom operator's system, email address (if connected via POP3, SMTP or IMAP4) and if connected to webmail system form mail.ru, yandex.ru, rambler.ru, gmail.com, yahoo.com and many others, user's phone number, IMEI, IMSI, MAC address of user's equipment and ICQ UIN. The third part of SORM is therefore quite comprehensive in coverage. The main agency for implementing the mandate under SORM series falls with Roskomnadzor which is Russia's main agency for surveillance and now includes internet surveillance in its functional area.

2. International Control of Internet: Internet Corporation for Assigned Names and Numbers (ICANN) has for long controlled Internet through control of IP addresses, Domain Name system (DNS)[23] and Root servers. The body is incorporated under the law of state of California, USA and so is subject to USA's law. Although USA declared in 2014 that it was not going to extend contract with ICANN which had allowed US Department of Commerce to control the former through power of oversight. USA has been promoting multistakeholder model of governing Internet which has not found enthusiastic audience in Russia. This is

[23] See Chapter 4

because Russia has found that representation of diverse state and non-state actors is not enough to mitigate USA’s domineering presence in operation of Internet. Apart from greater role in ICANN, it wants control over distribution system that connects domain names like .ru to the domain name system of the global Internet. In line with vision of cyberspace, it along with China, Tajikistan and Uzbekistan had proposed to the UN Secretary General some points to enhance international control of internet to promote control over sovereign information space among member states. This has been given document titled ‘International Code of Conduct for Information Security’.[24] This proposal titled so has emphasized sovereignty over information space, political independence, threats from information weapons, use of information technology for terrorist, secessionist and extremist activities, and for causing disturbance, sabotage. The document has promoted compliance with domestic laws and building a culture of information security in which UN plays a role in peaceful settlement of international disputes in information sphere.

3. Russia is engaged in diplomacy to iron out cyber issues with number of countries. However, the pact that it has signed with China has features like agreement to not conduct cyber attacks against each other, jointly counteracting technology that destabilize the internal environment and exchange of information between agencies that ensures security of information infrastructure.
4. Russia has developed its own draft Convention on International Information Security that is heavy on the side of promoting cooperation between states in the sphere of information security. Thirteen out of 23 articles in this are regarding information security issues like information warfare among states, military conflict in information space, information technologies used by terrorists and confidence building measures in military use of information space. The draft Convention also calls for taking legislative or other steps to establish its jurisdiction over any criminalized and socially dangerous action in the information sphere perpetrated in the territory of the State, on board a vessel flying the flag of that and on board a plane or any other aircraft registered under the laws of that State. The Convention clearly strengthens the right of state actors over information space. The word sovereignty is mentioned in many places in the draft

[24] See Chapter 4

Convention. It also mentions increasing the use of information technology for warfare involving both state and non-state actors.

5. On the domestic front, Russia has put in place in certain laws to regulate number of activities in the cyberspace. First among these is a law to fight online piracy. This law is called Federal Law No. 187-FZ, dated July 2, 2013 on Amending Certain Legislative Acts of the Russian Federation on Issues of protecting Intellectual Rights in Information Telecommunications Networks'. It allows right holder of intellectual property like notion pictures and television films to file an application with the federal executive governmental body concerned, for restricting access to the information resources that have been disseminated online without their permission. The second law which has been brought is most popularly called the 'blogging law'. This came into force on August 2014. According to this, the popular bloggers are required to register with the state media surveillance and regulatory body Roskomnadzor, disclose their identity, and follow the same rules that journalists are required to follow in conventional state-registered mass media. A popular blogger has been defined under the law as someone whose page page attracts at least 3000 readers every day. Other restrictions that have been introduced are the demand to verify information before publishing and abstaining from releasing reports that contain slander, hate speech, extremist calls or other banned information. The bloggers are also banned fromusing obscene language, making heavy, drawing heavy criticism and mockery from the online crowd. Roskomnadzor has also made it clear that the rules under the law were not to be affected by the physical location of the web author because everyone writing in Russian and targeting Russian audience had to comply with the rules or else their content was bound to be blocked on the Russian territory. There is heavy fine for violation of the law. The third important law that has been introduced is the Federal Law No. 242 FZ which deals with data protection. This law requires personal data operators to store and process any personal data of Russian individuals within databases[25] located in Russia. More specifically, the law requires that database server to be located in the Russian territory. This has been possibly done to better control the data of citizens and tighten the grip over the information sphere of the country. Then in 2012, a law

[25] For definition of database and related concepts see Chapter 4, p.

was made that would compel Internet service providers and web hosting companies to block access to sites that feature sexual abuse of children, offer details about how to commit suicide, drug use and sites that solicit children for pornography. The list of banned sites will be managed by Roskomnadzor and is to be updated daily.

The points mentioned above bring forth Russia's position on a number of cyberspace related issues that have come up with increasing innovation in use of cyberspace for various purposes. The position points towards Russia's inclination to view cyberspace as a zone that can no longer be left out of the purview of control by state. It is not ungovernable nor should cyberspace be left ungovernable. The regulatory measures, be it the law on blacklisting some sites, or the one requiring database server in the country or the law on intellectual property rights or the law on bloggers, show that Russia is actively regulating the cyberspace. The targets have been the content people read, see and share. Secondly, Russia has kept state's internal and external threats at the heart of its most policies in regulating cyberspace. The law on bloggers is aimed at keeping a check on use of blogs to fuel discontent. The database related law is meant to ensure that data related to Russian individuals should remain in the country to prevent it getting used elsewhere in a manner that can pose national security threat. In international sphere, Russia's stance on giving more control in the hands of states for regulating one's sovereign space amply makes it clear that it does not consider cyberspace ungovernable for protecting one's sovereign interests. In enunciating such, Russia has received backing from some of its neighbours and certainly has allies in countries that are regulating cyberspace in various degrees. If this is placed in context of many instances of surveillance in other countries (like in USA, India, UK, Germany, Iran, Saudi Arabia, Iraq, Brazil), drawing up laws to protect online rights (like in USA) or blocking sites to protect children (like in Australia), then Russia finds partners in regulating cyberspace. The country has in addition to all this given a primary role to state to incorporate cyberspace in information warfare tools. This would entail unprecedented level of control of cyberspace by the state, giving heft to the first hypothesis.

But what are the factors that have gone into development of Russia's stance on cyberspace governance? The second hypothesis has attributed this to the surging online political activism and cyber crimes. Cyber crimes is a broad category which includes apart from regular hacking and identity theft, the disruption of systems by malwares, snooping on citizens by non-state actors that may be acting at the behest of state actor/s, disruption by attacks on websites, activities that undermine valuable intellectual property rights and activities in cyberspace that undermine polity and are meant to cause political destabilization. There are following facts that give substantial support to the argument that cyber political activism has caused worry in the government:

1. In 2010, Alexei Navalny, the famous Russian blogger, revealed through his blog that there was corruption in the East Siberian Pacific pipeline matter. Specifically, he alleged that the state controlled oil Pipeline Company Transneft embezzled approximately $4 billion in public funds in transactions connected to East Siberian Pacific pipeline. The internal audit of the company which had been done in 2007 had been published only in part. Navalny published the full audit report indicating the embezzlement. The details spread fast through his blog which showed Transneft documents. The details indicted that company's executives had used contracts with bogus subcontractor companies to siphon off cash into offshore bank accounts. The blog attracted thousands of comments. The same blogger also exposed the malpractices in Russian Parliamentary elections by posting videos of the wrong methods to win that were resorted to by the ruling party. Although he was arrested, the impact that the expose was intended to make had already been made. The videos went viral in social networking sites Vkonatakte and Facebook . It did not end here. The wife of the arrested blogger took up the twitter feed of her husband and videos of the protest spread fast. Many people pledged online to join the protests against the government. When the election results were out and the ruling party was found to be ahead, the reaction of many turned into disgust. Putin who was Prime Minister at that time, who is considered number two in the government in Russia, became the target of the protests because of his heavyweight personality. The social media during this time played important role in giving links to videos showing the malpractice. Russian government too responded online. None other than the then President Dmitri Medvedev responded by tweeting in which criticized Navalny. The other major crisis which the online political activism was the Euromaidan protests in Ukraine. The then Ukrainian

President Victor Yanukovych, who was negotiating with EU a trade agreement. The success of the agreement would have meant joining Western camp. Russia responded by stopping all goods from Ukraine and it had a sobering impact on Ukraine which started going slow on negotiations. After sometime, a chill fell over the talks and Ukraine demanded that EU compensate the loss for dip in trade with CIS which would naturally result from the agreement. It was around this time that twitter feed called Euromaidan (Euro meant Europe and Maidan referred to Freedom Square in Kiev) was formed. This feed was used to feed anti Yanukovych sentiments and to coordinate organization of protests in Euromaidan. From twitter, the word spread to Vkontakte. Pavel Durov, who was Vkontakte chief at the time, faced pressure from Federal agencies to hand over details of the protest organizers. He refused to comply citing that Russian jurisdiction did not extend to the protesters in Ukraine. The events had shown that social media had become a place to protest.

2. Even in copyright matters, Russia has relatively less known players like Pirate Party that describes itself libertarian and is against copyrights. They, in reaction to increasing discussions on protecting copyrights online, blocked visitors from IP addresses that belonged to state agencies or pro-copyright lobby.
3. The presence of American companies Twitter, Google and Facebook in Russia and their role in fuelling protests added an external dimension to the online political activism.

The above facts have a direct bearing on the nature of regulations that have been introduced and Russia’s stance on developing cyberspace for protecting one’s sovereign information space. The Russian stance on information warfare, protection of country’s information sphere, protection of data of its citizens and preventing use of internet to fuel domestic discontent and destabilizing tendencies have seemingly arisen out of the recent incidents in which cyber crimes and online political activism played a key role. The second hypothesis therefore too seems to be bolstered with the facts that have been collected. In the context of overall Invention-Innovation-Practices-Entrenchment framework, it can be put in the following ways: Use of internet for committing theft, accessing resources and goods for free (music, art, entertainment), online political activism, cyber warfare,

are all innovations of internet that have occurred due to human machine interface. These innovations have fuelled certain practices and have attracted governments like that of Russia to regulate by means of laws, rules and even by mastering it by putting it use (like in information warfare). In fact, mastering a technology is the most subtle yet most direct way of controlling cyberspace.

5.3 Recent Developments

Russia has gained prominence in matters of cyberspace. Apart from its cyber pact with China, its role in putting cyber security in deliberations in BRICS has gained attention. In the Ufa declaration of BRICS in 2015, Russia and China have reinforced call for greater multilateral control of Internet. Also, in the most recent US presidential elections, there was strong Russian mark when it was suspected that Russian hackers had hacked some sites to reveal details that would weaken the credibility of Democratic Presidential candidate Hillary Clinton. In hindsight, many even find the Russian connection credible as Donald Trump emerged victorious pulling off greatest upset. These new events too reinforce the two hypotheses that the study has put. The world in fact is moving towards a set up in which state is the focal point of governing cyberspace and Russia is the main wheel in this trend. Its advocacy of such system is not reflected in what is happening in Russia but is now present in what other countries are also doing.

5.4 Areas that can be developed further

This study has not taken into consideration biometrics. However, biometrics is controlled by governments. So, in all likelihood, inclusion of biometrics is unlikely to weaken either of the two hypotheses. In fact, biometrics is used in most countries to secure the country and to keep record of all citizens- an exclusively government domain. However, it remains to be seen how Deep Web’s study would change the study’s main conclusions because a large part of Deep Web is unexplored much like depths of ocean. It is believed to be used by all those who prefer strict anonymity. It is used by all sorts of people-criminals like drug dealers, assassins, scientists, journalists for secret investigations, intelligence people and organizations and several others. Accessible through Tor (The Onion Router), which was originally developed by US Naval Research Laboratory, the communication is perfectly confidential and only certain vulnerabilities can be exploited to reveal someone. Therefore, it is not very much under the government control. The important thing is that much of the traffic one sees in Internet today is only tip of the iceberg. A lot lies beneath in Deep Web and state's potential role in that part of the Web would be helpful in analyzing cyberspace further.

Appendix 1: Russia-China Cyber Pact

Government of the Russian Federation

On April 30, 2015 No. 788-p

Moscow

On signing the Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in ensuring international information security.

In accordance with paragraph 1 of Article 11 of the Federal Law "On international treaties of the Russian Federation", Russian Foreign Ministry submitted to approve coordinated with other federal bodies of executive power and pre-crafted with the Chinese side a draft agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in the field of International Information Security (attached).

Instruct the Russian Foreign Ministry to hold talks with the Chinese side and on reaching an agreement to sign on behalf of the Government of the Russian Federation said Agreement, allowing making the annexed draft changes without principle.

Prime Minister

The Russian Federation Dmitry Medvedev

Contents : Chapter III Definition

Between the Government of the Russian Federation and the Government of the People's Republic of China Cooperation in the field of international information security.

Government of the Russian Federation and the Government of People's Republic of China, hereinafter referred to as the Parties Guided by the provisions of the Treaty of Good Neighbourliness and Friendly Cooperation between the Russian Federation and China Republic of July 16, 2001,

Noting the significant progress in the development and introduction of new information and communication technologies, which form the global information space,

Attaching great importance to the role of information and communication technology in promoting economic and social development for the benefit of all humanity and the maintenance of international peace, security and stability,

Expressing concern threats related to possible use of such technologies in the civil and military spheres in order, not compatible with the objectives of international peace, security and stability, in order to undermine the sovereignty and security of State and interference in their internal affairs and violation of privacy of citizens, destabilize the political and socio-economic environment, kindling ethnic and religious hatred, Attaching great importance to the international information security as one of the key elements of the international security,

Reaffirming that the sovereignty and international rules and principles derived from the state sovereignty applies to the conduct of States in activities related to the use of information and communication technology, and the jurisdiction of States over information infrastructure in their territory, and that the state has the sovereign right to define and implement public policies on matters relating to information and telecommunications network “Internet”, including security,

Emphasizing the joint work within the framework of the Shanghai Cooperation Organisation,

Convinced that the further deepening of trust and development of cooperation between the Parties in the field of information and communication technologies are imperative, and in their interest,

Taking into account the important role of information security to ensure the fundamental rights and freedoms of man and citizen,

Attaching great importance to the balance between security and human rights in the field of information and communication technologies,

In order to prevent threats to international information security, to ensure the interests of the Parties in order to create an international information environment, which is characterized by peace and cooperation,

Trying to form a multilateral, transparent and democratic international system of management information and telecommunications network “Internet” in order to control the internationalization of information and telecommunications network “Internet” and equal rights of states to participate in the process, including the democratic governance of the main resources of information and telecommunications network “Internet” and their equitable distribution,

Desiring to create a legal and institutional framework for cooperation of the Parties in the field of international information security,

Have agreed as follows:

Article 1

Basic Concepts

For the purposes of interaction between the Parties in the implementation of this Agreement, the basic concepts, the list of which is given in annex, which is an integral part of this Agreement. The said application may be supplemented, as necessary, refined and updated by agreement of the Parties.

Article 2

The main threats in the field of international information security

In the implementation of cooperation under this Agreement, the Parties believe that the main threats to international information security are the use of information and communication technologies:

1. to carry out acts of aggression aimed at the violation of the sovereignty, security, territorial integrity of States and a threat to international peace, security and strategic stability;
2. for the application of economic and other damage, including through the provision of a destructive impact on the objects of the information infrastructure;
3. for terrorist purposes, including for the promotion of terrorism and involvement in terrorist activities and more supporters;
4. to commit offenses and crimes, including those related to unauthorized access to computer data;
5. to interfere in the internal affairs of States, violations of public order, incitement of ethnic, racial and religious hatred, propaganda of racist and xenophobic ideas and theories that give rise to hatred and discrimination, incitement to violence and instability, as well as to destabilize the internal political and socio-economic situation, violation of government;
6. for the dissemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States.

Article 3

Key areas of cooperation

1. In view of the major threats referred to in Article 2 of this Agreement, the Parties authorized representatives and the competent authorities of the Parties, which are determined in accordance with Article 5 of this Agreement, shall cooperate in ensuring international information security in the following areas:

1) definition, coordination and implementation of the necessary cooperation in ensuring international information security;
2) establishment of channels of communication and contacts with a view to jointly respond to threats in the sphere of international information security;
3) cooperation in the development and promotion of international law in order to ensure national and international information security;
4) joint response to the threats in the field of international information security as defined in Article 2 of this Agreement;
5) the exchange of information and cooperation in law enforcement to investigate cases involving the use of information and communication technologies for terrorist and criminal purposes;
6) the development and implementation of the necessary joint confidence building measures that contribute to ensuring international information security;
7) Cooperation between the competent authorities of the parties to ensure the safety of the critical information infrastructure of the Parties, technology exchange and cooperation between the competent authorities of the Parties in the field of Computer Emergency Response;

8) the exchange of information on the legislation of the Parties on issues of information security;
9) to contribute to improving the international legal framework and practical mechanisms of cooperation of the Parties in ensuring international information security;
10) the creation of conditions for cooperation between the competent authorities of the Parties in order to implement this agreement;
11) To enhance cooperation and coordination among State Parties on issues of international information security within the framework of international organizations and for a (including the United Nations, the International Telecommunication Union, the International Organisation for Standardisation, the Shanghai Cooperation Organization, the BRICS countries, the Regional Forum of the Association of South-East Asian security and other);
12) The promotion of research in the field of international information security, joint research work;
13) Joint training of specialists, exchange of students and teachers from specialized higher education institutions;
14) Conduct of meetings, conferences, seminars and other forums, delegates and experts of the Parties in the field of international information security;
15) The establishment of a mechanism for cooperation between the competent authorities of the Parties for the exchange of information and sharing of information on existing and potential risks, threats and vulnerabilities in the area of information security, their identification, assessment, research, mutual information about them and to prevent their occurrence.

2. The Parties or the competent authorities of the Parties may, by mutual agreement to define other areas of cooperation.

Article 4

General principles of cooperation

1. The Parties shall cooperate in the field of ensuring international information security in the framework of this Agreement in such a way that such cooperation contributed to social and economic development, it is compatible with the maintenance of international peace, security and stability, and consistent with generally recognized principles and norms of international law including the principles of peaceful settlement of disputes and conflicts, non-use or threat of force, non-interference in internal affairs, respect for human rights and fundamental freedoms and the principles of bilateral cooperation and non-interference in the information resources of the Parties
2. The activities of the Parties under this Agreement shall be consistent with the right of each Party to seek, receive and impart information, bearing in mind that such a right can be restricted by the legislation of the Parties in order to ensure national security.
3. Each Party shall have an equal right to protection of information resources of their state against misuse and unauthorized intervention, including by cyber attacks on them.

   Each Party shall not with respect to the other Party of such actions and assist the other Party in implementing this law.

Article 5

Basic forms and mechanisms of cooperation

1. Practical cooperation in specific areas of cooperation under this Agreement, the Parties may carry out by the competent authorities of the Parties responsible for the implementation of this Agreement. Within 60 days of the entry into force of this Agreement, the Parties will exchange through diplomatic channels the data on competent authorities of the Parties responsible for the implementation of this Agreement.
2. In order to create the legal and institutional framework for cooperation in specific areas of the competent authorities of the Parties may enter into appropriate agreements interdepartmental character.
3. The procdedure for the exchange defined in subparagraph 15 of paragraph 1 of Article 3 of this Agreement, as well as used for this message formats and means of protection of information transmitted are determined by corresponding agreements between the competent authorities of the Parties.
4. In order to review the implementation of this Agreement, exchange information, analysis and joint assessment of emerging threats to information security, as well as the determination to harmonize and coordinate a joint response to such threats Parties shall hold consultations on a regular basis, and authorized representatives of the competent authorities of the Parties. Consultations are carries out by agreement of the Parties, usually two times a year, alternately in the Russian Federation and the People's Republic of China. Each of the Parties may initiate additional consultation, offering the time and place of their implementation, as well as the agenda.

Article 6

Data protection

1. The Parties shall ensure adequate protection of transmitted or created in the course of cooperation under this Agreement, the information to which access is limited and distribution in accordance with the legislation of the Parties. Protection of such information in accordance with the legislation and (or) the relevant regulatory legal acts of the receiving Party. Such information shall not be disclosed, is not transferred without the written consent of the Party, which is the source of this information, and duly designated in accordance with the legislation of the Parties.
2. Protection of State Secrets of the Russian Federation and (or) protection of state secrets of China in the course of cooperation under this Agreement shall be performed in accordance with the Agreement between the Government of the Russian Federation and the Government of the People's Republic on mutual protection and ensure the safety of classified information by 24 May 2000 year, as well as the legislation and (or) the relevant regulatory legal acts of the Parties.

Article 7

Funding

1. The parties shall bear their own costs of participation of their representatives, and experts in the relevant measures for the implementation of this Agreement.

2. In respect of other costs associated with the execution of this Agreement, the Parties in each case may agree on a procedure for funding in accordance with the legislation of the Parties.

Article 8

Relation to other international agreements

This Agreement shall not affect the rights and obligations of the Parties under other international treaties to which it is a state, and not directed against any third country.

Article 9

Dispute Resolution

The parties shall resolve disputes that may arise in connection with the interpretation or application of this Agreement through consultation and negotiations between authorities of the Parties and if necessary, through diplomatic channels.

Article 10

Final Provisions

1. This Agreement is concluded for an indefinite period and shall enter into force on the 30th day following the date of receipt through diplomatic channels of the last written notification on fulfillment by the parties of internal procedures necessary for its entry into force.
2. The parties may make changes to this Agreement, which by mutual agreement of the Parties executed a separate protocol.
3. This Agreement may be terminated at the expiration of 90 days from receipt of one of the Parties through diplomatic channels, written notice to the other Party of its intention to terminate this Agreement.
4. In the event of termination of this Agreement, the Parties shall take measures to fullu implement the obligations to protect information and ensure compliance with previously agreed joint activities, projects and other activities carried out under this Agreement and not completed at the time of termination of this Agreement.

Done at, “” 2015, in duplicate, in the Russian and Chinese languages, both texts being equally authentic.

For the Government of Russian federation For Government of People’s Republic of China

Appendix to the Agreement between Government of the Russian Federation and the Governement of the People’s Republic of China on cooperation in ensuring international information security.

Basic Concepts used for the purposes of interaction between Parties in implementation of the Agreement between the Government of the Russian Federation and Government of the People’s Republic of China on cooperation in ensuring international information security.

“Information security”- a state of security for the individual, society, the state and its interests from threats, destructive and other negative impacts in the information space.

“Information infrastructure”- activities associated with the creation, transformation, transmission, use, storage of information has an impact, including on individual and social consciousness, information infrastructure and information itself.

“Information resources”-information infrastructure, as well as proper information and its flows.

“Information security”-a complex of legal, organizational and technical measures aimed at ensuring the integrity (immutability), privacy, and access to information.

“Objects of the critical information infrastructure”- information and telecommunication networks of public authorities;

information systems, information and telecommunication networks and automated process control systems operating in the defense industry, health, transport, communication, credit and finance, energy, fuel industry, nuclear industry, aerospace industry, mining industy, metallurgical industry and chemical industry.

“Cyber attacks”- purposeful action program (software and hardware) tools for information systems, information and telecommunication networks, telecommunication networks and automated process control systems, carried out for the purpose of impairment (termination) of their operations and (or) a security breach of information processed.

“The misuse of information resources”- the use of information resources without the appropriate license or in violation of the rules of the law of each of the Parties or international law.

“Unauthorized interference in information resources”- undue influence on the processes of creating, processing, conversion, transmission, use, storage information.

“Security threats”- factors that create a risk for the individual, society, the state and its interest in the information space.

Source: URL: http://www.theregister.co.uk/2015/05/11/russia_china_cyber_pact_social_media/

Appendix 2

European Convention on Cybercrime

Budapest, 23.XI.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalization, convergence and continuing globalization of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interest in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to defer action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalization of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R(85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Minsiters support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient systems of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I-Use of terms

Article 1-Definitions

For the purposes of this Convention:

a. “computer system” means any device or a group of interconnected or related or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
b. “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
c. “service provider” means:
i. any public or private entity that provides to users of its users of its service the ability to communicate by means of a computer systems, and
ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.
d. “traffic data” means any computer data relating to a communication by means of a computer scan, generated by a computer system that formed a part in the chain of communication origin, destination, route, time, date, size duration, or type of underlying service.

Chapter II- Measures to be taken at the national level

Section 1-Substantive criminal law

Title 1- Offences against the confidentiality, integrity and availability of computer data and systems

Article 2-Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4- Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5- System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as crimina

as criminal offences under its domestic law when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6- Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2- Computer-related offences

Article 7- Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8-Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right the causing of a loss of property to another person by:

a. any input, alteration, deletion or suppression of computer data,
b. any interference with the functioning of a computer system, with the fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3- Content-related offences

Article 9- Offences related to Child Pornography

1. Each Party adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
a. producing child pornography for the purpose of its distribution through a computer system;
b. offering or making available child pornography through a computer system;
c. distributing or transmitting child pornography through a computer system;
d. procuring child pornography through a computer system for oneself or for another person;
e. Possessing child pornography in a computer system or a computer data storage medium.
2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
a. a minor engaged in sexually explicit conduct;
b. a person appearing to be minor engaged in sexually explicit conduct;
c. realistic images representing a minor engaged in sexually explicit conduct.
3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under the 18 years of age. A Party may, however, require a lower age limit, which shall be not less than 16 years.
4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4-Offences related to infringements of copyright and related rights

Article 10-Offences related to infringements of copyright and related rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performer, Producers of Phonograms and Broadcasting Organisations (Rome Convention),

the Agreement on Trade-Related Aspects of Intellectual Property Rights and WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this Article.

Title 5- Ancillary liability and sanctions

Article 11- Attempt and aiding or abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.
3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12- Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a. a power of representation of the legal person;
b. an authority to take decisions on behalf of the legal person;
c. an authority to exercise control within the legal person.

2. In addition to the cases already provided for in paragraph 1 of this Article, each Party shall measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.
3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative
4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13- Sanctions and measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2-Procedural law

Title 1-Common provisions

Article 14-Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a. the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b. other criminal offences committed by means of a computer system; and

c. the collection of evidence in electronic form of a criminal offence.

3. (a). Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. (b) Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i. is being operated for the benefit of a closed group of users, and

ii. does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15- Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and other limitation of the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and

procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2- Expedited preservation of stored computer data

Article 16- Expedited preservation of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its closure. A Party may provide for such an order to be subsequently renewed.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for its domestic law.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17- Expedited preservation and partial disclosure of traffic data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 18- Production order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
3. For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a. the type of communication service used, the technical provisions taken thereto and the period of service;
b. the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4- Search and seizure of stored computer data

Article 19- Search and seizure of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a. a computer system or part of it and computer data stored therein; and
b. a computer-data storage medium in which computer data may be stored in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
3. Each Party shall adopt such legislative and other measures as may be necessary to empower it competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a. seize or similarly secure a computer system or part of it or a computer data storage medium;
b. make and retain a copy of those computer data;
c. maintain the integrity of the relevant stored computer data;
d. render inaccessible or remove those computer data in the accessed computer system.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5- Real-time collection of computer data

Article 20- Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a. collect or record through the application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability:

i. to collect or record through the application of technical means on the territory of that Party; or

ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21- Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a. collect or record through the application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability:

i. to collect or record through the application of technical means on the territory of that Party, or

ii. to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3- Jurisdiction

Article 22- Jurisdiction

1. Each Party shall adopt such legislative and other measure as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
   a. in its territory; or
   b. on board a ship flying the flag of that Party; or
   c. on board an aircraft registered under the laws of that Party; or
   d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III- International co-operation

Section 1- General principles

Title 1- General principles relating to international co-operation

Article 23- General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2- Principles relating to extradition

Article 24- Extradition

1 (a). This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided

that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

1 (b). Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraphs 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognize the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested party deems that it has jurisdiction over the offence, the requested Party shall submit the case at eh request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 (a). Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

7 (b). The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3- General principles relating to mutual assistance

Article 25- General principles relating to mutual assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
2. Each Party shall adopt such legislative and other means as may be necessary to carry out the obligations set forth in Articles 27 through 35.
3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.
4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.
5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26- Spontaneous information

1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.
2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4- Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27- Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists,

unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. (a). Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. (b). The central authorities shall communicate directly with each other; (c). Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; (d). The Secretary General of the Council of Europe shall set up and keep updated a registers of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.
3. Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.
4. The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b. it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.
6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.
7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.
8. The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
9. (a). In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. (b). Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). (c). Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. (d). Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the

requested Party. (e). Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28- Confidentiality and limitation on use

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
2. The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a. kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b. not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.
4. Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2- Specific provisions

Title 1- Mutual assistance regarding provisional measures

Article 29- Expedited preservation of stored computer data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.
2. A request for preservation made under the paragraph 1 shall specify:

a. the authority seeking the preservation;

b. the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c. the stored computer data to be preserved and its relationship to the offence;

d. any available information identifying the custodian of the stored computer data or the location of the computer system;

e. the necessity of the preservation; and

f. that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.
4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.
5. In addition, a request for preservation may only be refused if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b. the requested Party considers that the execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30- Expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path which the communication was transmitted.
2. Disclosure of traffic data under paragraph 1 may only be withheld if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

Title 2- Mutual assistance regarding investigative powers

Article 31- Mutual assistance regarding accessing of stored computer data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2. The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.
3. The request shall be responded to on an expedited basis where:

a. there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
b. the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32- Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorization of another Party:

a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33- Mutual assistance regarding the real-time collection of traffic data

1. The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.
2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34- Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communication transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3- 24/7 Network

Article 35- 24/7 Network

1. Each Party shall designate a point of contact available on a twenty four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or if implemented by its domestic law and practice, directly carrying out the following measures:

a. the provision of technical advice;
b. the preservation of data pursuant to Articles 29 and 30;
c. the collection of evidence, the provision of legal information, and locating f suspects.

2. (a). A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
   (b). If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate that it is able to co-ordinate with such authority or authorities on an expedited basis.
3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV- Final provisions

Article 36- Signature and entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.
2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.
4. In respect of any signatory State which subsequently expressed its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37- Accession of the Convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.
2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38- Territorial application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.
2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the

expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39- Effects of the Convention

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

a. the European Convention of Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
b. the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
c. the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.
3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40- Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that its avails itself of the possibility of requiring additional elements as provided for under Articles 2,3,6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41- Federal clause

1. A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.
2. When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.
3. With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such

States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42- Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation (s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43- Status and withdrawal of reservations

1. A party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary, the withdrawal shall take effect on such a later date.
2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.
3. The Secretary General of the Council of Europe may periodically enquire with parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44- Amendments

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.
2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.
3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by CDPC and, following consultation with the non-member States to this Convention, may adopt the amendment.
4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.
5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45- Settlement of disputes

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.
2. In case of a dispute between Parties as to the interpretation or application of this Convention; they shall seek a settlement of the dispute through negotiation or any

other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46: Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

a. The effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b. The exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c. Consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in cooperation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47: Denunciation

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48: Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention;

a. Any signature;

b. The deposit of any instrument of ratification, acceptance, approval or accession;

c. Any date of entry into force of this Convention in accordance with Articles 36 and 37;

d. Any declaration made under Article 40 or reservation made in accordance with Article 42;

e. Any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorized thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and In French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

Source:http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Appendix 3:

The Ministry of Foreign Affairs of Russia

Convention on International Information Security (Concept)

Preamble

The State Parties to the Convention,

Noting the considerable progress in the development of information and communication technologies and means that make up the information space,

Expressing their concerns about threats connected with the possible uses of these technologies and means for purposes not compatible with measures to ensure international security and stability, both in the military and the civilian spheres,

Understanding the importance of international information security as one of the key elements in the system of international security,

Confident that the further growth of trust and the development of cooperation between the States Parties on issues of international information security are essential and beneficial to all parties,

Taking into consideration the important role that information security plays in ensuring basic human rights and freedoms,

Taking into account the 8 December 2010 resolution A/RES/65/41 of the General Assembly of the United Nations "Developments in the field of information and telecommunications in the context of international security",

Striving to limit threats to international information security, ensure the information security of States Parties, and create an information space characterized by peace, cooperation, and harmony,

Desiring to create a legal and organizational basis for cooperation between the States Parties in the sphere of international information security,

Referring to the 20 November 2000 resolution A/RES/55/29 of the General Assembly of the United Nations "Role of science and technology in the context of international security and disarmament", in which, in part, it is stated that achievements in science and technology can be put to both civilian and military use, and that it is necessary to support and stimulate the development of science and technology for use in civilian activities,

Acknowledging the necessity of preventing possible uses of information and communication technology for purposes not compatible with ensuring international stability and security, and capable of having a negative effect on the integrity of governmental infrastructures, causing damage to their security, *stressing* the necessity of increasing the coordination and strengthening the cooperation between States in the struggle against the criminal use of information technology and noting the role the United Nations and other international and regional organizations can play in that context,

Stressing the importance of the secure, uninterrupted, and stable functioning of the Internet and the necessity of protecting the Internet and other information and communication networks from possible harmful actions vulnerability to threats,

Affirming the necessity for a common understanding of Internet security issues and further cooperation on the national and international level,

Affirming again that political authority in connection with governmental policy issues related to the Internet is a sovereign right of States, and that the governments of States have rights and responsibilities as regards governmental policy issues related to the Internet on an international level,

Acknowledging that trust and security when using information and communication technologies is a fundamental basis of the information society, and that it is necessary to stimulate, form, develop, and actively integrate a stable global culture of cybersecurity, as is noted in the 21 December 2009 resolution A/RES/64/211 of the General Assembly of the United Nations "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures",

Noting the necessity of activating efforts to overcome the "digital divide" by increasing the ease of supply of information and communication technology to developing countries, and increasing their potential in relation to cutting-edge practices and professional training in the sphere of cybersecurity, as is noted in the 21 December 2009 resolution A/RES/64/211 of the General Assembly of the United Nations "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures",

Convinced of the necessity of prioritizing the creation of a common policy aimed at protecting society against illegal actions in the information space, which will include passing corresponding legislation and strengthening international cooperation,

Recognizing the serious changes caused by the spread of digital technology, unification, and continuing globalization of computer networks,

Concerned about the threat that computer networks may also be used to commit crimes, and that the proof of such crimes may be kept in these networks and passed on within them,

Acknowledging the necessity of cooperation between governments and private business in the fight against illegal activity in the information space and the necessity of protecting the legal interests of parties involved in the use and development of information and communication technology, *Believing* that fighting illegal activity in the information space effectively requires international cooperation that is broader, more dynamic, and more efficient,

Convinced that this Convention is necessary in the fight against breeches of the confidentiality, integrity, and accessibility of computer systems and networks and computer information, as well as the misuse of such systems, networks, and information by ensuring the punishment of such actions, detailed in this Convention, and in the granting of sufficient authority to effectively fight such offenses through the tracking, exposure, and investigation of such offenses on an internal and international level, and through the development of agreements on efficient and reliable international cooperation,

Keeping in mind the necessity of ensuring the appropriate balance between maintaining law and order and protecting fundamental human rights, as foreseen in the 1966 International Covenant on Civil and Political Rights, as well as other international human rights agreements, which assert the right of each individual to freely hold his or her own ideas, and to freely express these ideas and opinions, including the freedom to seek, receive, and distribute any kind of information or idea, regardless of national borders,

Keeping in mind also the right to a private life and the protection of personal data,

Taking into account the 1989 United Nations Convention on the Rights of the Child, and the Convention concerning the prohibition and immediate action for the elimination of the worst forms of child labour, passed by the General Conference of the International Labour Organization in 1999,

Welcoming recent events enabling the further growth of international understanding and collaboration in the struggle against illegal activity in the information space, including measures undertaken by the United Nations, the Shanghai Cooperation Organization, the European Union, the Asia-Pacific Economic Cooperation organization, the Organization of American States, the Association of Southeast Asian Nations, the Organisation for Economic Co-operation and Development, the Group of Eight (G8), and other international organizations and forums, have agreed to the following:

Chapter 1. Main Clauses

Article 1. Subject and aim of the Convention

The subject that this Convention seeks to regulate is the activity of governments to ensure international information security.

The aim of this Convention is to act against the use of information and communication technology to violate international peace and security, as well as to set up measures ensuring that the activity of governments in the information space will:

1. further general social and economic development;

2. be carried out in such a way as to be compatible with efforts to support international peace and security;
3. correspond to generally accepted principles and norms of international law, including principles of peacefully regulating conflicts and disagreements, abstaining from the use of force, not interfering in internal issues, and respecting fundamental human rights and freedoms;
4. be compatible with the right of each individual to seek, receive, and distribute information and ideas, as is affirmed in UN documents, while keeping in mind that this right may be restricted through legislation to protect the national and social security of each State, as well as to prevent the wrongful use of and unsanctioned interference in information resources;
5. guarantee the free exchange of technology and information, while maintaining respect for the sovereignty of States and their existing political, historical, and cultural specificities.

Article 2. Terms and definitions

The following terms and definitions are used for this Convention:

1. "**access to information**" - the possibility of receiving and using information;
2. "**information security**" - a state in which personal interests, society, and the government are protected against the threat of destructive actions and other negative actions in the information space;
3. "**information warfare**" - conflict between two or more States in the information space with the goal of inflicting damage to information systems, processes, and resources, as well as to critically important structures and other structures; undermining political, economic, and social systems; carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents;
4. "**information infrastructure**" - the total complex of technical means and systems of the formation, conversion, transfer, use, and storage of information;
5. "**information system**" - the total amount of information stored in a database and the technology used to support the processing of that information;
6. "**information weapon**" - information technology, means, and methods intended for use in information warfare;
7. "**information space**" - the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself;
8. "**information and communication technologies**" - the total amount of methods, production processes, and programming and technical elements, integrated with the goal of forming, converting, transferring, using, and storing information;
9. "**information resources**" - an information infrastructure, as well as the information itself and the flow of that information;
10. "**confidentiality of information**" - the mandatory requirement that a party granted access to certain information will not transfer this information to a third party without the agreement of the owner;
11. "**critically important part of the information infrastructure**" - a part (element) of an information infrastructure, actions against which could have consequences

directly connected to national security, including the security of individuals, society, and the government;

12. "**international information security**" - a state of international relations that excludes the possibility of breaks in global stability or the creation of threats to the security of governments and the global community in the information space;
13. "**the misuses of information resources**" - the use of information resources without the necessary rights, or which involves a violation of existing regulations, national legislation, or international legal norms;
14. "**unsanctioned interference in information resources**" - illegal action affecting the processes of forming, processing, converting, transferring, using, and storing information;
15. "**information system operator**" - an individual citizen or corporation whose runs an information system, including the processing of information contained in its database;
16. "**illegal activity in the information space**" - the use of information resources and/or activity affecting them in the information space for illegal purposes;
17. "**presentation of information**" **-** actions aimed at the receipt of information by a certain group, or the transfer of information to a certain group;
18. "**dissemination of information**" **-** actions aimed at the receipt of information by an indefinite group, or the transfer of information to an indefinite group;
19. "**terrorism in the information space**" - the use of information resources and/or activity affecting them in the information space for the purposes of terrorism;
20. "**threat to the information space (threat to information security)**" - factors that pose a danger to individuals, society, and the state, and their interests, in the information space.

Article 3. Exceptions to the application of this Convention

This Convention will not apply in those cases when the actions in question are taken within the information infrastructure of one State, citizen, or corporation under the jurisdiction of that State, and the effects of those actions are only felt by citizens and corporations under the jurisdiction of that State, and no other State has grounds to assert its jurisdiction.

Article 4. The main threats to international peace and security in the information space

The following are seen as the main threats in the information space that could damage international peace and stability:

1. the use of information technology and means of storing and transferring information to engage in hostile activity and acts of aggression;
2. purposefully destructive behavior in the information space aimed against critically important structures of the government of another State;
3. the illegal use of the information resources of another government without the permission of that government, in the information space where those resources are located;
4. actions in the information space aimed at undermining the political, economic, and social system of another government, and psychological campaigns carried out against the population of a State with the intent of destabilizing society;

5. the use of the international information space by governmental and non-governmental structures, organizations, groups, and individuals for terrorist, extremist, or other criminal purposes;
6. the dissemination of information across national borders, in a manner counter to the principles and norms of international law, as well as the national legislation of the government involved;
7. the use of an information infrastructure to disseminate information intended to inflame national, ethnic, or religious conflict, racist and xenophobic written materials, images or any other type of presenting ideas or theories that promote, enable, or incite hatred, discrimination, or violence against any individual or group, if the supporting reasons are based on race, skin color, national or ethnic origin, or religion;
8. the manipulation of the flow of information in the information space of other governments, disinformation or the concealment of information with the goal of adversely affecting the psychological or spiritual state of society, or eroding traditional cultural, moral, ethical, and aesthetic values;
9. the use, carried out in the information space, of information and communication technology and means to the detriment of fundamental human rights and freedoms;
10. the denial of access to new information and communication technologies, the creation of a state of technological dependence in the sphere of informatization, to the detriment of another State;
11. information expansion, gaining control over the national information resources of another State.

Additional factors increasing the danger of the aforementioned threats are:

1. difficulty in identifying the source of hostile actions, especially taking into account the growing activity of individuals, groups, and organizations, including criminal organizations, which provide intermediary services, carrying out activities in the name of others;
2. the potential danger of the inclusion of undeclared destructive capabilities in information and communication technology;
3. the difference in the levels of information and communication technologies in use, and in their security, in different States ("digital inequality");
4. the difference in national legislation and practices as regards the formation of a secure and quickly restorable information infrastructure.

Article 5. Main Principles of Ensuring International Information Security

The information space belongs to humankind as a whole. Its security is instrumental in ensuring the sustainable development of global civilization.

To create and foster an atmosphere of trust in the information space, the States Parties must observe the following principles:

1. the activities of each State Party in the information space must promote social and economic development and must be consistent with the goals of maintaining world peace and security, and conform to the universally recognized principles and norms of international law, including the principles of peaceful reconciliation

of strife and conflict, of the non-use of force in international relations, of non-interference into the internal affairs of other States, and of respect for the sovereignty of States and the major human rights and freedoms;

2. as they shape the system of international information security, the States Parties shall be guided by the principle of indivisibility of security, which means that the security of each State is inextricably connected with the security of all other States and the international community as a whole and shall not strengthen their security at the expense of the security of other States;
3. each State Party must strive to overcome the disparity in the level of equipment of national information systems with modern information and communication technologies, to bridge the "digital divide" with the purpose of lowering the general threat level in the information space;
4. all States Parties in the information space enjoy sovereign equality, have equal rights and obligations and are possess equal rights as stakeholders in the information space irrespective of their economic, social, political and other differences;
5. each State Party has the right to make sovereign norms and govern its information space according to its national laws. Its sovereignty and laws apply to the information infrastructure located in the territory of the State Party or otherwise falling under its jurisdiction. The States Parties must strive to harmonize national legislation, the differences whereof must not create barriers on the road to a reliable and secure information space;
6. each State Party must observe the principle of responsibility for its own information space, including responsibility for its security and the nature of information it holds;
7. each State Party has the right to develop its information space without external interference and each other State must respect that right in accordance with the principle of equal rights and self-determination of peoples stipulated in the Charter of the United Nations;
8. each State Party, with consideration for the lawful interests in security of other States, may freely and independently determine its interests in the support of information security, on the basis of sovereign equality, as well as freely choose the methods by which it will ensure its own information security in accordance with international law;
9. the States Parties acknowledge that aggressive "information warfare" is a crime against international peace and security;
10. the information space of States Parties should not be the object of acquisition for other States as a result of threats of force or the use of force;
11. each State Party has the inalienable right to self-defense against aggressive actions against it in the information space, if the source of aggression can be reliably located and the retaliatory measures are appropriate;
12. each State Party will determine its military potential in the information space on the basis of national procedures, with consideration for the lawful interests in security of other States, as well as the necessity of working to strengthen international peace and security. No State Party will make an attempt to achieve dominance in the information space over other States;
13. a State Party may locate its forces and means of ensuring information security on the territory of another State in accordance with an agreement, developed by both parties on a voluntary basis through negotiations, and in accordance with international law;

14. each State Party will take the measures necessary to ensure that the activity of international information systems for the management of the flow of transport and finance, means of communication, means of international information exchange, including the exchange of information for scientific and educational purposes, continues without interference, based on the understanding that such interference could negatively affect the information space as a whole;
15. States Parties should support and stimulate scientific and technical developments connected with the exploration of the information space, as well as educational activity, aimed at forming a global culture of cybersecurity;
16. each State Party will, within the limits of its means, ensure that fundamental human rights and freedoms, and the rights and freedoms of citizens, and intellectual property laws, including patents, technologies, commercial secrets, brands, and copyrights, are adhered to in its information space;
17. each State Party guarantees freedom of speech and expression in its information space, as well as protection against illegal interference into the private lives of citizens;
18. each State Party aims to maintain a balance between fundamental human rights and the effective counteraction of terrorist use of the information space;
19. States Parties do not have the right to limit or interrupt the access of citizens to the information space, except when acting to protect national and social security, or when preventing the illegal use of an unsanctioned interference into their national information infrastructure;
20. States Parties stimulate the partnership between business and civil society in the information space;
21. States Parties acknowledge their responsibility to ensure that citizens, public and state bodies, other States, and the global community are informed about new threats to the information space and about known methods of increasing the level of their security.

Chapter 2. Main Measures For Averting And Resolving Military Conflict In The Information Space

Article 6. Main Measures for Averting Military Conflict in the Information space

Guided by the principles laid out in Article 5, the States Parties shall take steps to anticipate and expose potential conflicts in the information space and take joint action to avert them and resolve crises and disputes peacefully.

To this end, the States Parties shall:

1. cooperate to ensure international information security to maintain world peace and security and to contribute to global economic stability and progress, general welfare of the peoples of the world and discrimination-free international cooperation;
2. take all necessary steps to prevent any destructive information action originating from their own territory or using the information infrastructure under their jurisdiction, as well as cooperate to locate the source of computer attacks carried

out with the use of their territory, to repel these attacks and to eliminate their consequences;

3. refrain from developing and adopting plans or doctrines capable of increasing threats in the information space, straining relations between States or provoking "information wars";
4. refrain from any actions aimed at a complete or partial breach of the integrity of the information space of another State;
5. refrain from using information and communication technology to interfere with the internal affairs of another State;
6. refrain, in international relations, from threatening to use or using force against the information space of any other State with the purpose of breaching it or as a means of resolving conflict;
7. refrain from organizing or encouraging the organization of any irregular forces with the purpose of carrying out unlawful activities in the information space of another State;
8. refrain from slander as well as from using insulting or hostile propaganda to intervene into or interfere in the internal affairs of other States;
9. have the right and duty to take action against the proliferation of untruthful or distorted messages which could be considered as a means of interfering in the internal affairs of other States or as damaging world peace and security;
10. take action aimed at limiting the proliferation of "information weapons" and the technology for their creation.

Article 7. Measures for Resolving Military Conflict in the Information Space

1) The States Parties shall resolve conflicts in the information space primarily by means of negotiation, investigation, mediation, reconciliation, arbitration, court trial, appeal to regional bodies or agreements, or by other peaceful means of their choice so as not to endanger world peace and security.
2) In any international conflict, the right of the States Parties that are involved in the conflict to choose the means of "information warfare" is limited by applicable norms of international humanitarian law.

Chapter 3. Main Measures For Preventing The Use Of The Information Space For Terrorist Purposes

Article 8. The Use of the Information space for Terrorist Purposes

The States Parties acknowledge the possibility of the information space being used for carrying out terrorist activities.

Article 9. Main Measures for Preventing the Use of the Information space for Terrorist Purposes

To prevent the use of the information space for terrorist purposes, the States Parties shall:

1. take action to prevent the use of the information space for terrorist purposes and acknowledge the necessity of decisive joint efforts to this end;

2. strive to work out uniform approaches to disabling Internet resources of a terrorist nature;
3. acknowledge the need for establishing and expanding the exchange of information on possible computer attacks, on the signs, facts, methods, and means of using the Internet for terrorist purposes, and on the goals and activities of terrorist organizations in the information space, as well as the need for the exchange of experience and best practices on monitoring Internet resources, finding and monitoring the content of websites of a terrorist nature, carrying out criminal investigations by computer experts in this sphere, and legal regulation and the organization of activities for preventing the use of the information space for terrorist purposes;
4. take such steps of legislative or other nature as may be necessary to allow law enforcement authorities to carry out investigative and other relevant activities aimed at preventing and suppressing terrorist activities in the information space and at the elimination of the consequences thereof, as well as at punishing persons and organizations guilty of conducting them;
5. take necessary steps of legislative or other nature which will guarantee lawful access to specific parts of the information and communication infrastructure in the territory of the State Party, which are legally implicated in being employed for the perpetration of terrorist activities in the information space or involved in such activities elsewhere, for the perpetration of activities conducive to terrorist acts, or for the activities of terrorist organizations or groups, or individual terrorists.

Chapter 4. MAIN MEASURES FOR COUNTERACTING ILLEGAL ACTIVITY IN THE INFORMATION SPACE

Article 10. Main Measures for Counteracting Illegal Activity in the Information space

To counteract illegal activity in the information space, the States Parties shall:

1. strive to criminalize the use of information resources and/or the manipulation of them in the information space for unlawful purposes, which include the unauthorized dissemination of information, breaches of confidentiality, and damaging the integrity or accessibility of information, and also take legislative or other steps to stipulate the responsibility and hold responsible persons for perpetrating, attempting, being accomplices in or instigating criminalized and socially dangerous actions in the information space;
2. take legislative or other steps to ensure that offenders in the information space receive effective, proportional, and convincing punishment.

Article 11. Measures on Organizing Criminal Procedures

To organize criminal procedures, the States Parties shall:

1. take legislative or other steps to stipulate powers and procedures for the purposes of conducting individual criminal investigations or court trials in cases of the perpetration of criminalized and socially dangerous actions in the information space;

2. ensure the stipulation, execution, and application of powers and procedures for the purposes of conducting individual criminal investigations or court trials in cases of the perpetration of criminalized and socially dangerous actions in the information space in compliance with the provisions and guarantees provided for by the legislation of the State and ensuring the appropriate level of the protection of human rights and freedoms, as well as with the principle of proportionality.
3. take legislative or other steps enabling the law enforcement authorities of the State to take swift action for the protection of certain data, including data on information flows stored in the information and communication infrastructure, when there are reasons to believe that these data are especially vulnerable to loss or manipulation;
4. take legislative or other steps to guarantee timely access of the law enforcement authorities of the State or a person appointed by these authorities to sufficient amounts of data on information flows as to identify service providers and the route of a specific message in its information space;
5. take legislative or other steps which may be necessary to empower the law enforcement authorities of the State to search or gain similar access to information and communication systems and their parts and the data stored therein, as well as to storage media which may contain the data in question, in its territory, and to other data and information and communication systems of their information space which are reasonably implicated in storing the data in question;
6. take legislative or other steps which may be necessary to empower the law enforcement authorities of the State to demand from a person present in its territory and possessing information on the functioning of the relevant information and communication system, its means of protection and the data stored therein, the release of this information, which would allow these authorities to take action, within the scope of their authority, for the purpose of carrying out individual criminal investigations or court trials in cases of the perpetration of criminalized and socially dangerous actions in the information space;
7. take legislative or other steps which may be necessary to empower the law enforcement authorities of the State to collect or record information by means of technology in its territory as well as to demand similar action from service providers carried out continuously and in cooperation with the law enforcement authorities of the States;
8. take legislative or other steps to establish its jurisdiction over any criminalized and socially dangerous action in the information space perpetrated in the territory of the State, on board a vessel flying the flag of that State, and on board a plane or any other aircraft registered under the laws of that State.

   If jurisdiction over an alleged offence is claimed by more than one State Party, the interested parties hold consultations to decide on the most suitable jurisdiction for prosecution.

Chapter 5. International Cooperation In The Sphere Of International Information Security

Article 12. Cooperation between the States Parties

1. The States Parties shall cooperate with each other according to the provisions of this Convention and through other international agreements.
2. The States Parties shall, on the basis of voluntariness and reciprocity, exchange best practices on the prevention, legal investigation, and the liquidation of consequences of crimes, including those related to terrorism, involving the information space. The State Party has the right to request that the information it provides be kept confidential. The State Party that receives such information has the right to refer to it when discussing issues of mutual assistance with the State that provided it.

Article 13. Confidence-Building Measures in the Sphere of the Military Use of the Information space

Each State Party must strive to promote confidence-building measures in the sphere of the military use of the information space, which include:

1. the exchange of national security concepts in the information space;
2. timely exchange of information on crises and threats in the information space and on the steps taken to deal with them;
3. consultations on activities in the information space which may raise concerns of States Parties and cooperation on resolving conflicts of military nature.

Article 14. Consultative Assistance

The States Parties shall cooperate with and consult each other on any issues related to the goals or the implementation of the provisions of this Convention.

Closing Provisions

Article 15. Signing of the Convention

This Convention shall be open for signature by all States.

Article 16. Ratification of the Convention

This Convention is subject to ratification. Instruments of ratification shall be deposited with the Secretary-General of the United Nations.

Article 17. Accession to the Convention

This Convention shall remain open for accession by any State. The instruments of accession shall deposited with the Secretary-General of the United Nations.

Article 18. Entering into Force

1. This Convention shall enter into force on the thirtieth day following the date of deposit of the twentieth instrument of ratification or accession with the Secretary-General of the United Nations.
2. For each State ratifying or acceding to this Convention after the deposit of the twentieth instrument of ratification or accession, this Convention shall enter into force on the thirtieth day after the deposit of the instrument of ratification or accession by such State.

Article 19. Amending the Convention

1. Any State Party may propose an amendment and present it to the Secretary-General of the United Nations. The Secretary-General then forwards the proposed amendment to the States Parties requesting them to specify whether they are in favor of holding a conference of States Parties to consider and vote on the proposals. If, within four months of the date of this communication, at least one-third of the States Parties speak in favor of such a conference, the Secretary-General holds this conference under the auspices of the United Nations. Any amendment passed by the majority of the States Parties represented at the conference and taking part in the vote shall be submitted for approval by the General Assembly.
2. An amendment passed in accordance with paragraph 1 of this article shall enter into force after it is approved by the General Assembly of the United Nations and passed by a two-thirds majority of the States Parties.
3. When the amendment enters into force, it becomes binding for the States Parties that passed it, while the other States Parties remain bound by the provisions of this Convention and any previous amendments passed by these States.

Article 20. Reservations to the Convention

1. The Secretary-General of the United Nations receives and forwards to all parties the texts of reservations made by the States at the time of their ratification or accession.
2. A reservation that is incompatible with the goals and objectives of the Convention is not permitted.
3. Reservations may be withdrawn at any time by notification to the Secretary-General of the United Nations, who then notifies the other States. This notification enters into force on the date on which it is received by the Secretary-General of the United Nations.

Article 21. Denunciation of the Convention

Any State Party may denounce this Convention by written notification to the Secretary-General of the United Nations. The denunciation shall take effect one year following the date on which the notification is received by the Secretary-General.

Article 22. Depositary of the Convention

The Secretary-General of the United Nations shall be appointed as the depositary of this Convention.

Article 23. The original of this Convention, of which the Arabic, Chinese, English, French, Russian and Spanish texts are equally authentic, shall be deposited with the Secretary-General of the United Nations.

IN WITNESS WHEREOF, the undersigned, being duly authorized thereto by their respective Governments, have signed this Convention.

Source: https://cryptome.org/2014/05/ru-international-infosec.htm

***Primary Sources**

Aaron, Chris (2012), "The Growing Cyber-Security Market", RUSI Defence Systems Summer: 86-87, [Online: Web] accessed. URL: https://www.rusi.org/downloads/assets/RDS_201206_Aaron.pdf

ABC News (2007), "Conroy announces mandatory internet filters to protect children", December 31, 2007, [Online: Web] accessed. URL: http://www.abc.net.au/news/2007-12-31/conroy-announces-mandatory-internet-filters-to/999946

Acılar, Ali; Maxim Markin; Elena Nazarbaeva (2012), "Exploring the Digital Divide: A Case of Russia and Turkey", *International Journal of Innovation in the Digital Economy*, 3(3): 35-46.

Ackerman, Spencer (2014), "Snowden: NSA accidentally caused Syria's internet blackout in 2012", *The Guardian*, August 13, 2014, [Web: Online] accessed. URL: http://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war

Adams, James (2001), "Virtual Defense", *Foreign Affairs,* 80(3): 98-112.

Adler, Patdzricia and PeterA. Adler (2008), "The Cyber Worlds of Self-Injurers: Deviant Communities, Relationships, and Selves", *Symbolic Interaction*, 31 (1): 33-56.

Addley, Esther and Josh Halliday (2010), "WikiLeaks supporters disrupt Visa and MasterCard sites in Operation Payback", *The Guardian*, December 9, 2010, [Online: Web] accessed. URL: http://www.theguardian.com/world/2010/dec/08/wikileaks-visa-mastercard-operation-payback

Agence France-Presse (2013), “Microsoft, Nokia file EU complaint against Google over bundling its services with Android”, *NDTV Gadgets*, April 9, 2013, [Online: Web] accessed. URL: http://gadgets.ndtv.com/mobiles/news/microsoft-nokia-file-eu-complaint-against-google-over-bundling-its-services-with-android-351907

Alkalimat,Abdul (2004), *The African American Experience in Cyberspace: A Resource Guide to the Best Websites on Black Culture and Histor*, London: Pluto Press.

Apps, Peter (2014), “Estonia exercise shows NATO’s growing worry about cyber attacks”, *Reuters*, May 27, 2014, [Online: Web] accessed. URL: http://uk.reuters.com/article/2014/05/27/us-nato-cybercrime-exercise-idUKKBN0E72D120140527

Arrington, Michael (2006), “AllOfMP3 Responds to RIAA’s $ 1.65 Trillion Lawsuit”, *TechCrunch*, December 27, 2006, [Online: Web] accessed. URL: http://techcrunch.com/2006/12/27/allofmp3-responds-to-riaas-165-trillion-lawsuit/

Ashford, Warwick (2011), “London Conference on Cyberspace: securing the future of the internet”, *Computer Weekly*, November 2, 2011, [Online: Web] accessed. URL: http://www.computerweekly.com/news/2240106470/London-Conference-on-Cyberspace-securing-the-future-of-the-internet

Aspray, William and Paul E. Ceruzzi (2008), *The Internet and American Business*, Cambridge, Massachussetts, London: The MIT Press.

Azzi, Abderrahmane (1999), “Islam in Cyberspace: Muslim Presence on the Internet”, *Islamic Studies*, 38 (1): 103-117.

Babeo, Tony (1995), “The Debate over Teledemocracy”, *The Sloping Halls Review*, Paper 22, [Online: Web] Accessed, URL: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1013&context=shr.

Backer, Larry Catá (2008), “Global Panopticism: States, Corporations, and the Governance Effects of Monitoring Regimes”, *Indiana Journal of Global Legal Studies*, 15 (1): 101-148.

Banks, Michael A. (2008), *On the way to the Web: The Secret History Of the Internet and Its Founders*, Apress, Berkeley.

Barak, Azy (eds.) (2008), Psychological *Aspects of Cyberspace: Theory, Research*, *Applications*, New York: Cambridge University Press.

Barlow, John Perry (1996), “A Declaration of the Independence of Cyberspace”, [Online: Web] Accessed, URL: https://projects.eff.org/~barlow/Declaration-Final.html.

Barrett, Oliver Boyd (2006), “Cyberspace, globalization and empire”, *Global Media and Communication*, 2(1): 21-41.

BBC News (2013), “US-China cyber security working group meets”, July 9, 2013, [Online: Web] accessed. URL: http://www.bbc.com/news/world-asia-china-23177538

BBC News (2013), “President Obama upbraids China over cyber attacks”, March 13, 2013, [Online: Web] accessed. URL: http://www.bbc.com/news/world-us-canada-21772596

BBC News (2013), “US-China cyber security working group meets”, July 9, 2013, [Online: Web] accessed. URL: http://www.bbc.com/news/world-asia-china-23177538

BBC News (2010), “Russia checks claims of $ 4bn oil pipeline scam”, November 17, 2010, [Online: Web] accessed. URL: http://www.bbc.com/news/world-europe-11779154

Benkler, Yochai (2006), *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, New Haven and London, Yale University Press.

Berkman, Fran (2014), “Net neutrality jargon explained”, *Daily.com*, September 5, 2014, [Online: Web] accessed. URL: http://www.dailydot.com/politics/net-neutrality-glossary-terms/

Bernoff, Josh (2010), “The Splinternet War: Apple vs. Google vs. Facebook”, *DigitalNext*, April 30, 2010, [Online: Web] accessed. URL: http://adage.com/article/digitalnext/digital-marketing-apple-google-facebook/143619/

Biegel, Stuart (2001), *Beyond Our Control?:Confronting the Limits of Our Legal System in the Age of Cyberspace,* London, England: The MIT Press.

Bimber, Bruce (1998), “The Internet and Political Transformation: Populism, Community, and Accelerated Pluralism”, *Polity*, 31 (1): 133-160.

Birnbaum, Michael (2014), “Facebook blocks Russian page supporting Navalny, Putin’s biggest critic”, *The Washington Post*, December 20, 2014, [Online: Web] accessed. URL: http://www.washingtonpost.com/world/facebook-blocks-russian-page-supporting-navalny-putins-biggest-critic/2014/12/20/a8c782b8-8877-11e4-abcf-5a3d7b3b20b8_story.html

Brandom, Russell (2014), “Project Goliath: Inside Hollywood’s secret war against Google”, The Verge, December 12, 2014, [Online: Web] accessed. URL: http://www.theverge.com/2014/12/12/7382287/project-goliath

Brito, Jerry and Tate Watkins (2012), “Cyberwar is the New Yellowcake”, *Wired*, February 14, 2012, [Online: Web] accessed. URL: http://www.wired.com/2012/02/yellowcake-and-cyberwar/

Budd, John M. and Douglas Raber (1996), “Discourse Analysis: Method and Application in the Study of Information”, *Information Processing & Management*, 32 (2): 217-226, 1996.

Busch, Richard (2013), “Movie Studios Win Important Appeal Against File Sharing Giant isoHunt”, *Forbes*, March 1, 2013, [Online: Web] accessed. URL: http://www.forbes.com/sites/richardbusch/2013/04/01/movie-studios-win-important-appeal-against-bittorrent-giant-isohunt/

Chang, Andrea (2014), “Tech leaders lash out at government’s electronic spying”, *LA Times*, October 8, 2014, [Online: Web] accessed. URL: http://www.latimes.com/business/la-fi-silicon-valley-nsa-20141009-story.html

Cohn, Cindy, et al (2012), “Human Rights and Technology Sales: How Corporations Can Avoid Assisting Repressive Regimes”, *Electronic Frontier Foundation*, April 2012, [Online: Web] accessed. URL: https://www.eff.org/files/filenode/human-rights-technologsalesy-.pdf

Colin, Nicolas and Henri Verdier (2014), “The fight for digital sovereignty: industrial factors”, *Paris Tech Review*, June 30, 2014, [Online: Web] accessed. URL: http://www.paristechreview.com/2014/06/30/digital-sovereignty/

Corrons, Luis (2010), “4chan Users Organize Surgical Strike Against MPAA”, *Panda Media Center*, September 17, 2010, [Online: Web] accessed. URL: http://www.pandasecurity.com/mediacenter/malware/4chan-users-organize-ddos-against-mpaa/

Crews Jr., Clyde Wayne (2001), "One Internet is Not enough", *Cato Institute*, April 11, 2001, [Online: Web] accessed. URL: http://www.cato.org/publications/techknowledge/one-internet-is-not-enough

Croft, Adrian (2011), "London Conference on Cyberspace Seeks International Cooperation in Fighting Cyber Crime", *Reuters*, November 1, 2011, [Online: Web] accessed. URL: http://www.huffingtonpost.com/2011/11/01/london-conference-on-cyberspace_n_1069331.html?ir=India

Jiao, Wu (2014), "Xi: Respect cyber sovereignty", *China Daily USA*, July 17, 2014, [Online: Web] accessed. URL: http://usa.chinadaily.com.cn/epaper/2014-07/17/content_17818027.htm

Trend Micro (2013), "Latin American and Caribbean Cybersecurity Trends and Government Responses", May 2013, Washington, D.C.: OAS Secretariat for Multidimensional Security, [Online: Web] accessed. URL: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf

Wortham, Jenna (2012), "With Twitter, Blackouts and Demonstrations, Web Flexes Its Muscle", *The New York Times*, January 18, 2012, [Online: Web] accessed. URL: http://www.nytimes.com/2012/01/19/technology/protests-of-antipiracy-bills-unite-web.html?pagewanted=all

The Huffington Post (2012), "Wikipedia Blackout: 11 Huge Sites Protest SOPA, PIPA On January 18", January 18, 2012, [Online: Web] accessed. URL: http://www.huffingtonpost.com/2012/01/17/wikipedia-blackout_n_1212096.html?ir=India

Higgins, Parker, et al (2014), "Who has your back? Protecting Your Speech from Copyright and Trademark Bullies", An Electronic Frontier Foundation Report, October 27, 2014, Electronic Frontier Foundation, [Online: Web] accessed. URL: https://www.eff.org/files/2014/10/27/who-has-your-back-2014-copyright-trademark_0.pdf

Coleman, Gabriella (2014), "What It's Like to Participate in Anonymous' Actions", The Atlantic, December 10, 2010, [Online: Web] accessed. URL: http://www.theatlantic.com/technology/archive/2010/12/what-its-like-to-participate-in-anonymous-actions/67860/

McMilan, Robert (2014), "What Everyone Gets Wrong in the Debate Over Net Neutrality", *Wired*, June 23, 2014, [Online: Web] accessed. URL: http://www.wired.com/2014/06/net_neutrality_missing/

Walker, Craig (2014), "Weekend Read: Startup Innovation Requires Net Neutrality", The Accelerators, *Wall Street Journal*, August 22, 2014, [Online: Web] accessed. URL: http://blogs.wsj.com/accelerators/2014/08/22/weekend-read-innovation-requires-net-neutrality/

Ward, Mark (2012), "Anti-Sec: Who are the world's most wanted hackers?", BBC News, March 30, 2012, [Online: Web] accessed. URL: http://www.bbc.com/news/technology-17548704

McCoy, Terrence (2014), "Vladimir Putin hates everything about the Internet except 'Website Vladimir'", *The Washington Post*, April 25, 2014, [Online: Web] accessed. URL: http://www.washingtonpost.com/news/morning-mix/wp/2014/04/25/vladimir-putin-hates-everything-about-the-internet/

Yeung, Ken (2013), "US State Department to host Google+ 'Hangouts at State' series to discuss the nation's foreign policy", *The Next Web*, April 15, 2013, [Online: Web] accessed. URL: http://thenextweb.com/insider/2013/04/15/us-state-department-to-host-google-hangouts-at-state-series-that-cover-the-nations-foreign-policy/

Leyden, John (2015), “Russia and China seal cyber non-hack pact”, *The Register*, May 11, 2015, [Online: Web] accessed. URL: http://www.theregister.co.uk/2015/05/11/russia_china_cyber_pact_social_media/

Daly, John C.K. (2006), “US Air Force Prepares For Cyber Warfare”, Space Daily, October 9, 2006, [Online: Web] accessed. URL: http://www.spacedaily.com/reports/US_Air_Force_Prepares_For_Cyber_Warfare_999.html

Doward, Jamie and Robert Lewis (2012), “UK ‘exporting surveillance technology to repressive nations’”, *The Guardian*, April 7, 2012, [Online: Web] accessed. URL: http://www.theguardian.com/world/2012/apr/07/surveillance-technology-repressive-regimes

Zittrain, Jonathan (2014), “No, Barack Obama Isn’t Handling Control of the Internet Over to China”, *The New Republic*, March 24, 2014, [Online: Web] accessed. URL:http://www.newrepublic.com/article/117093/us-withdraws-icann-why-its-no-big-deal

Landler, Mark and David E. Sanger (2013), “U.S. Demands China Block Cyberattacks and Agree to Rules”, *The New York Times*, March 11, 2013, [Online: Web] accessed. URL: http://www.nytimes.com/2013/03/12/world/asia/us-demands-that-china-end-hacking-and-set-cyber-rules.html?ref=asia&_r=0

Sanger, David E. (2013), “U.S. Blames China’s Military Directly for Cyberattacks”, The New York Times, May 6, 2013, [Online: Web] accessed. URL: http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?pagewanted=all&_r=0

Flynn, Sean, et al (2011), “Public Interest Analysis of the US TPP Proposal for an IP Chapter”, Draft Version 1.3, Program on Information Justice and Intellectual

Property, American University Washington College of Law, [Online: Web] accessed. URL: http://infojustice.org/wp-content/uploads/2011/12/TPP-Analysis-12062011.pdf

The Tor Project (2015), "Tor: Overview", [Online: Web] accessed. URL: https://www.torproject.org/about/overview.html.en

Market Watch (2014), "Top 20 Cyber Security Companies 2014", June 18, 2014, [Online: Web] accessed. URL: http://www.marketwatch.com/story/top-20-cyber-security-companies-2014-2014-06-18

Farnsworth, Timothy (2011), "China and Russia Submit Cyber Proposal", *Arms Control Today*, 41(9): 35-36.

Grisham, Lori (2015), "Timeline: North Korea and the Sony Pictures hack", USA Today Network, January 5, 2015, [Online: Web] accessed. URL: http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/

The Economist (2010), "A worm in the centrifuge", September 30, 2010, [Online: Web] accessed. URL: http://www.economist.com/node/17147818

Zeller Jr., Tom (2006), "The Internet Black Hole That is North Korea", The New York Times, October 23, 2006, [Online: Web] accessed. URL: http://www.nytimes.com/2006/10/23/technology/23link.html?_r=0

Meinrath, Sascha (2013), "The Future of the Internet: Balkanization and Borders", *Time.com*, October 11, 2013, [Online: Web] accessed. URL: http://ideas.time.com/2013/10/11/the-future-of-the-internet-balkanization-and-borders/

The Economist (2010), "A virtual counter-revolution", September 2, 2010, [Online: Web] accessed. URL: http://www.economist.com/node/16941635

Thompson, Derek (2010), "The Fall of the Internet and the Rise of the Splinternet", *The Atlantic*, March 8, 2010, [Online: Web] accessed. URL: http://www.theatlantic.com/business/archive/2010/03/the-fall-of-the-internet-and-the-rise-of-the-splinternet/37181/

Thompson, Clive (2014), "Today's epic battle has been fought before, when radio took to the air a century ago", Smithsonian, October 2014, [Online: Web] accessed. URL: http://www.smithsonianmag.com/innovation/debate-over-net-neutrality-has-its-roots-fight-over-radio-freedom-180952774/?no-ist

Sankin, Aaron (2014), "The Conservative Case Against Net Neutrality", *Daily.com*, May 16, 2014, [Online: Web] accessed. URL: http://www.dailydot.com/politics/net-neutrality-ted-cruz-fcc/

Teller, Tomer (2012), "The Biggest Cybersecurity Threats of 2013", Forbes.com, May 5, 2012, [Online: Web] accessed. URL: http://www.forbes.com/sites/ciocentral/2012/12/05/the-biggest-cybersecurity-threats-of-2013-2/2/

Ramli, David (2014), "Telstra backs online piracy", www.afr.com, September 2, 2014, [Online: Web] accessed. URL: http://www.afr.com/p/technology/telstra_backs_online_piracy_crackdown_Xaj6EfkspduePC1kGCWOSK

McGuire, David (2005), "At a Glance: MGM v.Grokster", *The Washington Post*, March 28, 2005, [Online: Web] accessed. URL: http://www.washingtonpost.com/wp-srv/technology/articles/groksterprimer_033805.htm

Kobrin, Stephen J. (2001), "Territoriality and the Governance of Cyberspace", *Journal of International Business Studies*, 32(4): 687-704.

Myszewski, Dave (2003), “Cyberlibertarianism in the Silicon Valley”, Stanford Review, 31(5), [Online: Web] accessed. URL: http://stanfordreview.org/old_archives/Archive/Volume_XXXI/Issue_5/News/news4.shtml

Leyden, John (2010), “Spanish entertainment industry feels wrath of Anonymous”, *The Register*, October 7, 2010, [Online: Web] accessed. URL: http://www.theregister.co.uk/2010/10/07/anonymous_ent_biz_ddos_hits_spain/
Downes, Larry (2011), “SOPA: Hollywood’s latest effort to turn back time”, CNET.com November 1, 2011, [Online: Web] accessed. URL: http://www.cnet.com/news/sopa-hollywoods-latest-effort-to-turn-back-time/

*Letter to Senator Pat Leahy about S.968 (Protect IP Act) and H.R. 3261(Stop Online Piracy Act), November 15, 2011, [Online: Web] accessed. URL: http://politechbot.com/docs/sopa.google.facebook.twitter.letter.111511.pdf

Sofaer, Abraham D., et al (), “Cyber Security and International Agreements”,*Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, [Online: Web] accessed. URL: http://cs.brown.edu/courses/csci1800/sources/lec17/Sofaer.pdf

Rosen, Rebecca J. (2011), “So, Was Facebook Responsible for the Arab Spring After all?”, The Atlantic, September 3, 2011, [Online: Web] accessed. URL: http://www.theatlantic.com/technology/archive/2011/09/so-was-facebook-responsible-for-the-arab-spring-after-all/244314/

Schwartz, Mathew J. (2013), “Snowden Says U.S. Hacking Civilians Since 2009”, Dark Reading, June 13, 2013, [Online: Web] accessed. URL: http://www.darkreading.com/risk-management/snowden-says-us-hacking-chinese-civilians-since-2009/d/d-id/1110353?

Seoul Framework For and Commitment to Open and Secure Cyberspace (2013), [Online: Web] accessed. URL: https://www.dsci.in/node/1561

McCullagh, Declan (2011), “Senate bill amounts to death penalty for Web sites”, CNET.com, May 12, 2011, [Online: Web] accessed. URL: http://www.cnet.com/news/senate-bill-amounts-to-death-penalty-for-web-sites/

McDowall, Angus (2014), “Saudi Arabia warns women: Don’t join driving ban protest”, Haaretz, October 23, 2014, [Online: Web] accessed. URL: http://www.haaretz.com/news/world/1.622434

Sassen, Saskia (1998), “On the Internet and Sovereignty”, *Indiana Journal Of Global Legal Studies*, 5(2): 545-559.

World Summit on the Information Society (2003), “Declaration of Principles”, Geneva 2003, December 12, 2003, [Online: Web] accessed. URL: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|0

*Russia-China Cyber Security Agreement (2015) of April 30, 2015. Given in “Russia-China seal cyber non-hack pact”, by John Leyden, *The Register*, May 11, 2015, [Online: Web] accessed. URL: http://www.theregister.co.uk/2015/05/11/russia_china_cyber_pact_social_media/

Lucas, Edward (2014), “Russia’s information warfare”, European Voice, November 6, 2014, [Online: Web] accessed. URL: http://www.europeanvoice.com/article/russias-information-warfare/

RT (2014), “Russia, China prepare to sign unique cybersecurity treaty-report”, October 21, 2014, [Online: Web] accessed. URL: http://rt.com/politics/197812-russia-china-network-security/

Kommersant Daily (2014), “Russia and China to join forces as cyber superpowers”, October 21, 2014,[Online: Web] accessed. URL: http://www.russia-direct.org/russian-media/russia-and-china-join-forces-cyber-superpowers

*Roskomnadzor (2014), “Unlock torrent trackers-“centenarians” “anti-piracy” registry”, July 3, 2014, [Online: Web] accessed. URL: http://rkn.gov.ru/news/rsoc/news26096.htm

*Roskomnadzor (2014), “For four months Roskomnadzor found about 2500 websites that disseminate personal information of children”, September 1, 2014, [Online: Web] accessed. URL: http://rkn.gov.ru/news/rsoc/news26956.htm

*Roskomnadzor (2014), “Head of ROSKOMNADZOR feels certain that the Internet should be regulated by the international organisation”, November 21, 2014, [Online: Web] accessed. URL: http://rkn.gov.ru/news/rsoc/news28520.htm

*ICANN (2014), “ICANN Nominating Committee”, [Online: Web] accessed. URL: https://www.icann.org/resources/pages/nomcom-2013-12-13-en

Reporters without Borders (2014), “100 Information Heroes”, [Online: Web] accessed. URL: en.rsf.org

*Office of the Vice-President of United States of America Press Release (2009), “Remarks by Vice President Biden at 45th Munich Conference on Security Policy”, February 7, 2009, [Online: Web] accessed. URL: http://www.whitehouse.gov/the-press-office/remarks-vice-president-biden-45th-munich-conference-security-policy

*Office of President of President of United States of America Press Release, “Remarks by the President on Securing Our Nation’s Cyber Infrastructure”, May 29, 2009, [Online: Web] accessed. URL: http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

Oliphant, Roland (2014), “Facebook and Gmail face blacklist under Russian web laws”, *The Telegraph*, September 26, 2014, [Online: Web] accessed. URL: http://www.telegraph.co.uk/news/worldnews/europe/russia/11124089/Facebook-and-Gmail-face-blacklist-under-Russian-web-laws.html

Open Net Initiative (2015), “YouTube Censored: A Recent History”, [Online: Web] accessed. URL:https://opennet.net/youtube-censored-a-recent-history

Roettgers, Janko (2013), “RapidShare lays off most of its staff as it struggles to find new business model”, Gigaom.com, May 17, 2013, [Online: Web] accessed. URL: https://gigaom.com/2013/05/17/rapidshare-mass-layoffs/

Phadnis, Aditi (2012), “Putin visits India today Sistema issue on agenda”, Business Standard News, December 24, 2012, [Online: Web] accessed. URL: http://www.business-standard.com/article/economy-policy/putin-visits-india-today-sistema-issue-on-agenda-112122402030_1.html

Press TV (2014), “FBI cyber attacks a ‘violation of other nations’ sovereignty”, August 31, 2014, [Online: Web] accessed. URL: http://www.presstv.com/detail/2014/04/24/359925/us-violated-other-nations-sovereignty/

Poulsen, Kevin (2010), “PayPal Freezes WikiLeaks Account”, *Wired*, April 12, 2010, [Online: Web] accessed. URL: http://www.wired.com/2010/12/paypal-wikileaks/

Desk, Web (2015), “Pakistan tops list of most porn-searching countries: Google”, *The Express Tribune*, January 18, 2015, [Online: Web] accessed. URL: http://tribune.com.pk/story/823696/pakistan-tops-list-of-most-porn-searching-countries-google/

Winterford, Brett (2010), “Operation Payback directs DDoS attack at AFACT”, iTNEWS.com, September 28, 2010, [Online: Web] accessed. URL: http://www.itnews.com.au/News/233573,operation-payback-directs-ddos-attack-at-afact.aspx

Noman, Helmi (2011), "In the Name of God: Faith-Based Internet Censorship in Majority Muslim Countries", Open Network Initiative, August 1, 2011, [Online: Web] accessed. URL: https://opennet.net/sites/opennet.net/files/ONI_NameofGod_1_08_2011.pdf

Leena, N. (2011), "Cyber Crime Effecting E-commerce Technology", *Oriental Journal of Computer Science and Technology*, 4(1): 209-212, [Online: Web] accessed. URL: file:///C:/Users/shobhna/Downloads/OJCSV04I01P209-212%20(1).pdf

Google Official Blog (2013), "Secretary of State John Kerry kicks off "Hangouts at State" series on Google+", April 15, 2013, [Online: Web] accessed. URL: http://googleblog.blogspot.in/2013/04/secretary-of-state-john-kerry-kicks-off.html

Dinan, Stephen (2015), "Obama's State of the Union guests include illegal immigrant, gun violence victim, Ebola doctor", The Washington Times, January 19, 2015, [Online: Web] accessed. URL: http://www.washingtontimes.com/news/2015/jan/19/state-of-the-union-guests-include-illegal-immigran/

Gustin, Sam (2013), "NSA Spying Scandal Could Cost U.S. Tech Giants Billions", *Time.com*, December 10, 2013, [Online: Web] accessed. URL: http://business.time.com/2013/12/10/nsa-spying-scandal-could-cost-u-s-tech-giants-billions/

Noland, Marcus (2011), "Kim Jong-il's Denial of Service Attack", Peterson Institute for International Economics, May 8, 2011, [Online: Web] accessed. URL: http://blogs.piie.com/nk/?p=1153

Reporters Without Borders (2014), "New Global Coalition Urges Governments to Keep Surveillance Technologies in Check", April 4, 2014, [Online: Web] accessed. URL: http://en.rsf.org/new-global-coalition-urges-04-04-2014,46086.html

Fitzgerald, Drew (2014), “Net-Neutrality Debate Splits Telecom Industry”, Wall Street Journal, November 12, 2014, [Online: Web] accessed. URL: http://www.wsj.com/articles/net-neutrality-debate-splits-telecom-industry-1415833377

NETmundial (2014), “NETmundialMultistakeholder Statement”, April 24, 2014, [Online: Web] accessed. URL:

Gross, Grant (2014), “Net neutrality proposal could lead to broadband taxes, opponents say”, Computerworld, November 14, 2014, [Online: Web] accessed. URL: http://www.computerworld.com/article/2848452/net-neutrality-proposal-could-lead-to-broadband-taxes-opponents-say.html

Purkayastha, Prabir and Rishab Bailey (2014), “Multistakeholderism- a conduit for the corporate takeover of the Internet”, *Third World Resurgence*, July/August (287/288): 25-31. [Online: Web] accessed. URL: http://www.twnside.org.sg/title2/resurgence/2014/287-288/cover04.htm

Hariharan, Geetha (2014), “Multi-stakeholder Models of Internet Governance within States: Why, Who & How?”,*Centre for Internet & Society*, June 16, 2014, [Online: Web] accessed. URL: http://cis-india.org/internet-governance/blog/multi-stakeholder-models-of-internet-governance-within-states-why-who-how

Enigmax (2010), “MPAA Copy-Protected DRM Site Hacked by Anonymous”, TorrentFreak, October 15, 2010, [Online: Web] accessed. URL: http://torrentfreak.com/mpaa-copy-protected-drmsite-hacked-by-anonymous-101015/

Miller, Sean J. (2013), “MPAA Celebrates Court Victory Over Torrent Site”, Backstage, March 27, 2013, [Online: Web] accessed. URL: http://www.backstage.com/news/mpaa-celebrates-court-victory-over-torrent-site/

Ernesto (2010), “Movie Rental Outfit Hacked, Emails Leaked, Redirected to the Pirate Bay”, *TorrentFreak*, October 18, 2010, [Online: Web] accessed. URL: http://torrentfreak.com/movie-rental-outfit-hacked-emails-leaked-redirected-to-the-pirate-bay-101018/

Ernesto (2010), “Movie Rental Outfit Calls for Nationwide Pirate Bay Block”, *TorrentFreak,* September 16, 2010, [Online: Web] accessed. URL: http://torrentfreak.com/movie-rental-outfit-calls-fonationwider--pirate-bay-block-100916/

*Government of Russian Federation (2011), “Convention on International Information Security”, Ministry of Foreign Affairs, [Online: Web] accessed. URL: http://www.mid.ru/bdomp/ns-osndoc1e5f0de28fe77fdcc32575d900298676.nsf//7b17ead7244e2064c3257925003bcbcc!OpenDocument

Timberg, Craig (2013), “Major tech companies unite to call for new limits on surveillance”, *The Washington Post*, December 9, 2013, [Online: Web] accessed. URL: http://www.washingtonpost.com/business/technology/major-tech-companies-unite-to-call-for-new-limits-on-surveillance/2013/12/08/530f0fd4-6051-11e3-bf45-61f69f54fc5f_story.html

Losowsky, Andrew (2012), “Library.nu, Book Downloading Site, Targeted in Injunctions Requested by 17 Publishers”, The Huffington Post, February 16, 2012, [Online: Web] accessed. URL: http://www.huffingtonpost.com/2012/02/15/librarynu-book-downloading-injunction_n_1280383.html?ir=India

Lessig, Lawrence (1996), “The Zones of Cyberspace”, *Stanford Law Review*, 48 (5): 1403-1411.

Lessig, Lawrence and Robert W. McChesney (2006), “No Tolls on the Internet”, *The Washington Post*, June 8, 2006, [Online: Web] accessed. URL: http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060702108.html

Hill, Jonah Force (2014), “The Growth of Data Localization Post-Snowden: Analysis and Recommendations For U.S. Policymakers and Industry Leaders”, *Lawfare Research Paper Series*, 2(3): 1-41, [Online: Web] accessed. URL:

Rosenzweig, Paul (2014), “The Continuing Struggle for Control of Cyberspace-And The Deterioration of Western Influence”, *Lawfare*, January 13, 2014, [Online: Web] accessed. URL: http://www.lawfareblog.com/2014/01/the-continuing-struggle-for-control-of-cyberspace-and-the-deterioration-of-western-influence/

Morris, Adam (2013), “Julian Assange: The Internet threatens civilization”, *LA Review of Books*, May 1, 2013, [Online: Web] accessed from www.salon.com. URL: http://www.salon.com/2013/04/30/tk_5_partner_15/

Manne, Robert (2011), “Julian Assange: The Cypherpunk Revolutionary”, *The Monthly*, March 2011, [Online: Web] accessed. URL: http://www.themonthly.com.au/issue/2011/march/1324265093/robert-manne/cypherpunk-revolutionary

Wu, Tim (2003), “Network Neutrality, Broadband Discrimination”, Journal on Telecommunication and High Technology Law, Vol.2: 141-176, [Online: Web] accessed. URL: http://www.jthtl.org/content/articles/V2I1/JTHTLv2i1_Wu.PDF

Pickard, Victor (2007), “Neoliberal Visions and Revisions in Global Communications Policy From NWICO to WSIS”, Journal of Communication Inquiry, 31(2): 118-139, [Online: Web] accessed. URL:

Lewis, James A. (2010), “Multilateral Agreements To Constrain Cyberconflict”, *Arms Control Today*, 40 (5): 14-19.

Stiennon. Richard (2013), “IT Security Industry To Expand Tenfold”, *Forbes*, August 14, 2013, [Online: Web] accessed. URL: http://www.forbes.com/sites/richardstiennon/2013/08/14/it-security-industry-to-expand-tenfold/

Internet Ungovernance Forum (2014), September 4-5, 2014, [Online: Web] accessed. URL: https://iuf.alternatifbilisim.org/

Taylor, Stephen (2003), “Erosion of National Sovereignty by 21st Century Technology”, *International-Business-Center.com*, [Online: Web] accessed. URL: http://international-business-center.com/international_business_resources/Sovereignty.pdf

Feakin, Tobias (2012), “International cyber security: a divided road”, *The Strategist*, October 16, 2012, [Online: Web] accessed. URL: http://www.aspistrategist.org.au/international-cyber-security-a-divided-road/

Watanabe, Kohei (2013), “The Western Perspective in Yahoo! News and Google News: Quantitative analysis of geographic coverage of online news”, International Communication Gazette, 75 (2): 141-156.

Lunden, Ingrid (2015), “Intel Shuts down Russian Developer Forums to Comply with Russia’s ‘Blogger Law’”, *TechCrunch*, January 5, 2015, [Online: Web] accessed. URL: http://techcrunch.com/2015/01/05/intel-shuts-down-russian-developer-forums-to-comply-with-russias-blogger-law/

Markoff, John and Andrew E. Kramer (2009), “In Shift, U.S. Talks to Russia on Internet Security”, *New York Times*, December 12, 2009, [Online: Web] accessed. URL: http://www.nytimes.com/2009/12/13/science/13cyber.html?_r=0

Selyukh, Alina (2014), “ICANN chief: Russia, China will not hijack Internet oversight”, *Reuters*, April 2, 2014, [Online: Web] accessed. URL:

http://www.reuters.com/article/2014/04/02/us-usa-internet-domainnames-idUSBREA311SE20140402

Wei, Wang (2014), "How Russian Hackers Placed "Digital Bomb" Into the NASDAQ", *Hacker News*, July 20, 2014, [Online: Web] accessed. URL: http://thehackernews.com/2014/07/how-russian-hackers-placed-digital-bomb.html

Pomerantsev, Peter (2014), "How Russia is Revolutionizing Information Warfare", *The Atlantic*, September 9, 2014. Retrieved from *Defense One*, [Online: Web] accessed. URL: http://www.defenseone.com/threats/2014/09/how-russia-revolutionizing-information-warfare/93635/

Global Voices (2014), "How Not to Understand the Kremlin's Internet 'Kill Switch'", September 24, 2014, [Online: Web] accessed. URL:

Downes, Larry (2014), "How Netflix Poisoned the Net Neutrality Debate", *Forbes*, November 25, 2014, [Online: Web] accessed. URL: http://www.forbes.com/sites/larrydownes/2014/11/25/how-netflix-poisoned-the-net-neutrality-debate/

Dredge, Stuart (2013), "Hotfile to pay Hollywood studios $80m damages in filesharing settlement", *The Guardian*, December 4, 2013, [Online: Web] accessed. URL: http://www.theguardian.com/technology/2013/dec/04/hotfile-hollywood-filesharing-damages-mpaa

Kang, Cecilia (2011), "House introduces Internet piracy bill", *The Washington Post*, October 26, 2011, [Online: Web] accessed. URL: http://www.washingtonpost.com/blogs/post-tech/post/house-introduces-internet-piracy-bill/2011/10/26/gIQA0f5xJM_blog.html

Griffith, Justin (2011), "Hey Saudi Arabia-Abstinence only driver's education does not work", *Patheos.com*, December 4, 2011, [Online: Web] accessed. URL:

http://www.patheos.com/blogs/rockbeyondbelief/2011/12/04/hey-saudi-arabia-abstinence-only-drivers-education-does-not-work/

Jr. Perritt, Henry H. (1998), "The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance", Indiana Journal of Global Legal Studies, 5(2): 423-442.

Paganini, Pierluigi (2013), "Hactivism: Means and Motivations…What Else?",*InfoSec Institute*, October 2, 2013, [Online: Web] accessed. URL: http://resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else/

Ponemon Institute (2013), "The 2013 eCommerce Cyber Crime Report: Safeguarding Brand and Revenue This Holiday Season", Research Report, October 2013, [Online: Web] accessed. URL: http://www.emc.com/collateral/analyst-reports/h12493-ar-2013-ecommerce-cyber-crime-report.pdf

Deibert, Ronald J. and Masashi Crete-Nishihata (2012), "Global Governance and the Spread of Cyberspace Controls", *Global Governance: A Review of Multilateralism and International Organisations*, July-September, 18(3): 339-361, [Online: Web] accessed. URL: http://journals.rienner.com/doi/abs/10.5555/1075-2846-18.3.339

Thomas, Thomas K. (2012), "Google, Facebook should share revenue with us: Airtel", BusinessLine, July 20, 2012, [Online: Web] accessed. URL: http://www.thehindubusinessline.com/opinion/columns/thomas-k-thomas/google-facebook-should-share-revenue-with-us-airtel/article3662533.ece

Luhn, Alec (2014), "Google to close engineering office in Russia as internet restrictions bite", *The Guardian*, December 12, 2014, [Online: Web] accessed. URL: http://www.theguardian.com/world/2014/dec/12/google-closes-engineering-office-russia

Fields, James (2015), “Google Fiber turns up volume on net neutrality”, *Tennessean.com*, February 5, 2015, [Online: Web] accessed. URL: http://www.tennessean.com/story/money/2015/02/05/google-fiber-turns-volume-net-neutrality-debate/22890109/

*ICANN (2014), “About Generic Names Supporting Organisation”, April 23, 2014, [Online: Web] accessed. URL: http://gnso.icann.org/en/about

Kumar, Sangeet (2010), “Google Earth and the nation state: Sovereignty in the age of new media”, *Global Media and Communication*, 6(2): 154-176.

*Internet Engineering Task Force (2015), “Getting Started in the IETF”, [Online: Web] accessed. URL: http://www.ietf.org/newcomers.html#participation

*International Telecommunication Union (2005), “Report to the Council by ITU Secretary-General on the financial status of the World Summit on the Information Society as of April 5, 2005”, June 8, 2005, [Online: Web] accessed. URL: https://www.itu.int/wsis/docs2/funding/financial-status-wsis05.pdf

*International Telecommunication Union (2004), “Report to the Council by ITU Secretary-General on the financial status of the World Summit on the Information Society as of April 30, 2004, May 11, 2004, [Online: Web] accessed. URL: https://www.itu.int/wsis/docs2/funding/financial-status-wsis.pdf

Perry, Nick (2012), “Popular file-sharing website Megaupload shut down”, *USA Today*, January 20, 2012, [Online: Web] accessed. URL: http://usatoday30.usatoday.com/tech/news/story/2012-01-19/megaupload-feds-shutdown/52678528/1

*The White House Office of the Press Secretary (2013), “Fact Sheet: U.S.-Russian Cooperation on Information and Communications Technology Security”, June 17, 2013, [Online: Web] accessed. URL: https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol

Wolman, David (2013), “Facebook, Twitter Help the Arab Spring”, *Wired*, April 16, 2012, [Online: Web] accessed. URL: http://www.wired.com/2013/04/arabspring/

Mishra, Lalatendu and Sriram Srinivasan (2015), “Facebook launches Internet.org in India”, *The Hindu*, February 11, 2015, [Online: Web] accessed. URL: http://www.thehindu.com/business/Industry/facebook-launches-internetorg-in-india/article6879310.ece

Wagner, Ben (2012), “Exporting Censorship and Surveillance Technology”, Humanist Institute for Cooperation with Developing Countries, Hague, Netherlands, January 2012, [Online: Web] accessed. URL: https://hivos.org/sites/default/files/exporting_censorship_and_surveillance_technology_by_ben_wagner.pdf

Wagner, Ben and Claudio Guarnieri (2014), “German Companies Are Selling Unlicensed Surveillance Technologies to Human Rights Violators”, *Global Voices*, September 5, 2014, [Online: Web] accessed. URL: http://globalvoicesonline.org/2014/09/05/exclusive-german-companies-are-selling-unlicensed-surveillance-technologies-to-human-rights-violators-and-making-millions/

RT (2010), ““Anonymous” speaks out about WikiLeaks”, December 10, 2010, [Online: Web] accessed. URL: http://rt.com/usa/anonymous-wikileaks-hackers-assange/

Levs, Josh and Catherine E. Shoichet (2013), “Europe furious, ‘shocked’ by report of U.S. spying”, *CNN*, July 1, 2013, [Online: Web] accessed. URL: http://edition.cnn.com/2013/06/30/world/europe/eu-nsa/

Reporters without Borders (2014), “Enemies of the Internet”, March 12, 2014, [Online: Web] accessed. URL: http://12mars.rsf.org/wp-content/uploads/EN_RAPPORT_INTERNET_BD.pdf

Greenwald, Glenn, et al (2013), “Edward Snowden: the whistleblower behind the NSA surveillance revelations”, The Guardian, June 10, 2013, [Online: Web] accessed. URL: http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Phadnis, Shilpa (2013), “Edward Snowden sharpened his hacking skills in Delhi”, *The Times of India*, December 4, 2013, [Online: Web] accessed. URL: http://timesofindia.indiatimes.com/india/Edward-Snowden-sharpened-his-hacking-skills-in-Delhi/articleshow/26811526.cms

Dorling, Philip (2013), “Snowden reveals Australia’s links to US spy web”, *The Sydney Morning Herald*, July 8, 2013, [Online: Web] accessed. URL: http://www.smh.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html

Filiol, Eric and Robert Erra (2012), *Proceedings of the 11th European Conference on Information Warfare and Security, 5-6 July, 2012*, Reading, UK: Academic Publishing International Limited, [Online: Web] accessed.URL: http://academic-conferences.org/pdfs/ECIW_2012-Book.pdf

Robertson, Adi (2012), “Ebook download site library.nu shut down by coalition of international publishers”, *The Verge*, February 16, 2012, [Online: Web] accessed. URL: http://www.theverge.com/2012/2/16/2802060/library-nu-ifile-it-ebook-piracy-site-shut-down

Pillai, Sarath (2013), “DNS Root Servers: The most critical infrastructure on the internet”, *Slashroot.in*, October 15, 2013, [Online: Web] accessed. URL: http://www.slashroot.in/dns-root-servers-most-critical-infrastructure-internet

Karrenberg, Daniel (2005), "DNS Root Name Servers Frequently Asked Questions", *ISOC Member Briefing Series*, The Internet Society, Virginia, USA, [Online: Web] accessed. URL: https://www.isoc.org/briefings/020/

*Kruzel, John J. (2009), "Cybersecurity Poses Unprecedented Challenge to National Security, Lynn Says", *U.S. Department of Defense News*, June 15, 2009, [Online: Web] accessed. URL: http://www.defense.gov/news/newsarticle.aspx?id=54787

Brustein, Joshua (2014), "Darrell Issa's Internet Theory: Net Neutrality Will End Porn", *Bloomberg*, June 20, 2014, [Online: Web] accessed. URL: http://www.bloomberg.com/bw/articles/2014-06-20/darrell-issas-internet-theory-net-neutrality-will-end-porn

*Global Intellectual Property Center, U.S. Chamber of Commerce (2012), "Dangerous Fakes", [Online: Web] accessed. URL: http://www.theglobalipcenter.com/dangerous-fakes/

Ebert, Hannes and Tim Maurer (2013), "Cyberspace and the Rise of the BRICS", *Journal of International Affairs*, Columbia University, October 11, 2013, [Online: Web] accessed. URL: http://jia.sipa.columbia.edu/online-articles/cyberspace-rise-brics/

Dougherty, Patrick and Nadir Mechairia (2013), "Cyber Security in Greater Baltimore- A State of the Market Report", *Cyber Security 2013 Report: State of the Industry*, Economic Alliance of Greater Baltimore, July 24, 2013, [Online: Web] accessed. URL: http://www.greaterbaltimore.org/UploadedPdfs/CyberSecurity_Report.pdf

*ITU News (2013), "Cybersecurity takes centre stage", [Online: Web] accessed. URL: https://itunews.itu.int/en/3940-Cybersecurity-takes-centre-stage.note.aspx

Farivar, Cyrus (2011), “Cyber-security pits West against China, Russia”, *DW.DE*, November 1, 2011, [Online: Web] accessed. URL: http://www.dw.de/cyber-security-pits-west-against-china-russia/a-15502838

RT (2013), “Cyber war is US ‘red herring’ to put pressure on China”, June 8, 2013, [Online: Web] accessed. URL: http://rt.com/op-edge/china-us-cyber-war-393/

Carroll, Ward (2008), “Cyber War 2.0-Russia v. Georgia”, Defense Tech, [Online: Web] accessed. URL: http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/

PR Newswire (2004), “Cyber Security Industry Alliance Calls on the White House and Federal Agencies to Take Action on Twelve Steps to Improve Cyber Security and Enable Continued Innovation on the Internet”, December 7, 2004, [Online: Web] accessed. URL: http://www.prnewswire.com/news-releases/cyber-security-industry-alliance-calls-on-the-white-house-and-federal-agencies-to-take-action-on-twelve-steps-to-improve-cyber-security-and-enable-continued-innovation-on-the-internet-75715827.html

Hughes, Rex (2013), “Cyber Governance without Government”, Canada Centre for Global Security Studies, Munk School of Global Affairs, March 18, 2013, [Online: Web] accessed. URL: http://www.cyberdialogue.ca/2013/03/cyber-governance-without-government-by-rex-hughes/

8Convention On Cybercrime, Budapest (2001), Council of Europe, November 23, 2001, [Online: Web] accessed. URL: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Sriskandarajah, Dhananjayan (2014), “Corporate colonisation of cyberspace”, *Al-Jazeera English*, July 13, 2014, [Online: Web] accessed. URL: http://www.aljazeera.com/indepth/opinion/2014/07/corporate-colonisation-cyberspa-201471093456798730.html

Whyte, Christopher (2014), "Competition in Cyberspace: Why Russia's Anti-Piracy Hacking is Doomed to Fail", *Georgetown Journal of International Affairs*, August 4, 2014, [Online: Web] accessed. URL: http://journal.georgetown.edu/competition-in-cyberspace-why-russias-anti-privacy-hacking-is-doomed-to-fail/

Wan, William (2014), "Chinese President Xi Jinping takes charge of new cyber effort", *The Washington Post*, February 27, 2014, [Online: Web] accessed. URL: http://www.washingtonpost.com/world/chinese-president-takes-charge-of-new-cyber-effort/2014/02/27/a4bffaac-9fc9-11e3-b8d8-94577ff66b28_story.html

Sceats, Sonya (2015), "China's Cyber Diplomacy: a Taste of Law to Come?",*The Diplomat*, January 14, 2015, [Online: Web] accessed. URL: http://thediplomat.com/2015/01/chinas-cyber-diplomacy-a-taste-of-law-to-come/

Reuters (2014), "China says it's hard to resume cyber security talks with U.S.", October 19, 2014, [Online: Web] accessed. URL: http://www.reuters.com/article/2014/10/19/us-china-usa-cybersecurity-idUSKCN0I80GU20141019

Shi, Ting and Michael A. Riley (2014), "China Halts Cybersecurity Cooperation After U.S. Spying Charges", *Bloomberg*, May 20, 2014, [Online: Web] accessed. URL: http://www.bloomberg.com/news/articles/2014-05-20/china-suspends-cybersecurity-cooperation-with-u-s-after-charges

RT News (2014), "China demands end to US spying activities after new Snowden leak", March 24, 2014, [Online: Web] accessed. URL: http://rt.com/news/china-nsa-spying-reaction-869/

Deibert, Ron (2012), "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace", Canadian Defence & Foreign Affairs Institute, August 2012, [Online: Web] accessed. URL: https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf

Guevara, Inigo (2014), “Brazil designates torpedo, missile, cyber security, and more as strategic programmes”, *IHS Jane’s Defence Weekly*, December 1, 2014, [Online: Web] accessed. URL: http://www.janes.com/article/46576/brazil-designates-torpedo-missile-cyber-security-and-more-as-strategic-programmes

Lynch, Jennifer (2012), “From Finger Prints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond: A Special Report”, *Electronic Frontier Foundation*, May 2012, [Online: Web] accessed. URL: https://www.eff.org/files/filenode/biometricsimmigration052112.pdf

Reuters (2014), “Bharti Airtel to charge for using VoIP services”, December 24, 2014, [Online: Web] accessed. URL: http://in.reuters.com/article/2014/12/24/bharti-airtel-rates-idINKBN0K20SU20141224

Jackson, Peter (2010), “Meet USCybercom: Why the US is fielding a cyber army”, *BBC News*, March 15, 2010, [Online: Web] accessed. URL: http://news.bbc.co.uk/2/hi/technology/8511711.stm

Kravets, David (2014), “Bankrolled by broadband donors, lawmakers lobby FCC on net neutrality”, *ArsTechnica*, May 17, 2014, [Online: Web] accessed. URL: http://arstechnica.com/tech-policy/2014/05/bankrolled-by-broadband-donors-lawmakers-lobby-fcc-on-net-neutrality/

Riley, Duncan (2007), “Australia Joins China in Censoring the Internet”, *TechCrunch*, December 30, 2007, [Online: Web] accessed. URL: http://techcrunch.com/2007/12/30/australia-joins-china-in-censoring-the-internet/

RT News (2013), “Argentina, Brazil agree on cyber-defense alliance against US espionage”, September 15, 2013, [Online: Web] accessed. URL: http://rt.com/news/brazil-argentina-cyber-defense-879/

Hendry, Andrew and Darren Pauli (2008), “Appalled opposition hits back at Conroy’s Internet censorship”, *Computerworld*, October 24, 2008, [Online: Web] accessed. URL: http://www.computerworld.com.au/article/264974/_appalled_opposition_hits_back_conroy_internet_censorship/

Ward, Mark (2012), “Anti-Sec: Who are the world’s most wanted hackers?”,*BBC News*, March 30, 2012, [Online: Web] accessed. URL: http://www.bbc.com/news/technology-17548704

Cadwalladr, Carole (2012), “Anonymous: behind the masks of the cyber insurgents”, *The Guardian*, September 8, 2012, [Online: Web] accessed. URL: http://www.theguardian.com/technology/2012/sep/08/anonymous-behind-masks-cyber-insurgents

Leyden, John (2010), “Anonymous attacks PayPal in ‘Operation Avenge Assange’”, *The Register*, December 6, 2010, [Online: Web] accessed. URL: http://www.theregister.co.uk/2010/12/06/anonymous_launches_pro_wikileaks_campaign/

Saran, Samir and Abhijit Iyer-Mitra (2013), “Privacy, property and sovereignty in the cyber age”, *Observer Research Foundation*, October 8, 2013, [Online: Web] accessed. URL: http://www.observerindia.com/cms/sites/orfonline/modules/analysis/AnalysisDetail.html?cmaid=58031&mmacmaid=58032

Satpathy, Sambit (2014), “Airtel withdraws controversial VoIP data packs, puts the ball in TRAI’s court”, *BGR*, December 29, 2014, [Online: Web] accessed. URL: http://www.bgr.in/news/airtel-withdraws-controversial-voip-data-packs-puts-the-ball-in-trais-court/

India Today (2014), “Airtel to charge extra for VoIP calls, breaks net neutrality”, December 24, 2014, [Online: Web] accessed. URL: http://indiatoday.intoday.in/technology/story/airtel-to-charge-extra-for-voip-calls-breaks-net-neutrality/1/408635.html

Chock, Sasha Constanza (2013), “After Snowden: Towards Distributed Security in Cyberspace”, MIT Center for Civic Media, October 3, 2013, [Online: Web] accessed. URL: https://civic.mit.edu/blog/schock/after-snowden-towards-distributed-security-in-cyberspace

Technology Liberation Front (2014), “About the Technology Liberation Front”, *Techliberation.com*, [Online: Web] accessed. URL: http://techliberation.com/about/

Kaspersky Lab (2014), “About Kaspersky Lab”, [Online: Web] accessed. URL: http://www.kaspersky.co.in/about

Shubber, Kadhim (2013), “A simple guide to GCHQ’s internet surveillance programme Tempora”, *Wired*, June 24, 2013, [Online: Web] accessed. URL: http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101

Wortham, Jenna (2012), “A Political Coming of Age for the Tech Industry”, *The New York Times*, January 17, [Online: Web] accessed. URL: http://www.nytimes.com/2012/01/18/technology/web-wide-protest-over-two-antipiracy-bills.html?ref=technology

*International Telecommunication Union (2014), “World Summit On the Information Society+10 High Level Event Outcome Documents Geneva 2014”, [Online: Web] accessed. URL:

*United Nations Organisation (2011), “Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General”, *UN*

General Assembly 66th Session, Item 93 of the provisional agenda: Developments in the field of information and telecommunications in the context of international security, [Online: Web] accessed. URL: http://content.netmundial.br/files/67.pdf

*World Summit on the Information Society (2005), "Tunis Commitment", *Second Phase of the WSIS, 16-18 November 2005, Tunis*, [Online: Web] accessed. URL: http://www.itu.int/wsis/docs2/tunis/off/7.pdf

*World Summit on the Information Society (2005), "Tunis Agenda for the Information Society", *Second Phase of the WSIS, 16-18 November 2005, Tunis*, [Online: Web] accessed. URL: http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf

Marguiles, Peter (2013), "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", *Melbourne Journal of International Law*, Vol. 14, No. p.496, 2013, Roger Williams University Legal Studies Paper No. 155, [Online: Web] accessed. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2557517

Reardon, Marguerite (2014), "Comcast vs. Netflix: Is this really about Net neutrality", *CNET*, May 15, 2014, [Online: Web] accessed. URL: http://www.cnet.com/news/comcast-vs-netflix-is-this-really-about-net-neutrality/

Jordan, Tim and Paul Taylor (2004), *Hactivism and Cyberwars: Rebels With a Cause*, London, New York: Routledge.

Carey, Peter (2001), *The Internet and E-Commerce: A Specially Commissioned Report*, London: Thorogood.

Julie (2013), "4 Fascinating Facts on the Social Media Landscape in Russia", *Synthesio*, April 23, 2013, [Online: Web] accessed. URL: http://synthesio.com/corporate/2013/uncategorized/4-fascinating-facts-on-the-social-media-landscape-in-russia/#

International Intellectual Property Alliance (2012), “2012 Special 301 Report on Copyright Enforcement and Protection: Russian Federation”, February 10, 2012, [Online: Web] accessed. URL: http://www.iipa.com/rbc/2012/2012SPEC301RUSSIA.PDF

Parker, Emily (2014), “Can the Internet Defeat Putin?:AlekseiNavalny and Russia’s Protesters Face a Tough Battle”, *The New York Times*, December 30, 2014, [Online: Web] accessed. URL: http://www.nytimes.com/2014/12/31/opinion/aleksei-navalny-and-russias-protesters-face-a-tough-battle.html?_r=0

Reid, Ben (2006), “AllofMp3.com speak out over IFPI allegations”, *After Dawn*, June 6, 2006, [Online: Web] accessed. URL: http://www.afterdawn.com/news/article.cfm/2006/06/06/allofmp3_com_speak_out_over_ifpi_allegations

Marson, James (2013), “At E-Commerce Firms, Russia Rises”, *The Wall Street Journal*, November 12, 2013, [Online: Web] accessed. URL: http://www.wsj.com/articles/SB100014240527023048684045791917133955748l6

Keating, Joshua (2014), “Is Russia Really the Cybercrime Capital?”,*Slate*, August 6, 2014, [Online: Web] accessed. URL: http://www.slate.com/blogs/the_world_/2014/08/06/billion_password_hack_russian_hackers_aren_t_prolific_they_re_just_really.html

Nazdracheva, Lyudmila (2013), “Blogs begin to play a prominent political role”, *Russia Beyond The Headlines*, August 19, 2013, [Online: Web] accessed. URL: http://rbth.com/politics/2013/08/19/blogs_begin_to_play_a_prominent_political_role_29015.html

Zinovieva, Elena (2014), "Can Facebook win a bigger share of the Russian social media pie?",*Russia Direct*, February 4, 2014, [Online: Web] accessed. URL: http://www.russia-direct.org/analysis/can-facebook-win-bigger-share-russian-social-media-pie

Johnston, Casey (2015), "Crime, Punishment, and Russia's Original Social Network", *Motherboard*, February 12, 2015, [Online: Web] accessed. URL: http://motherboard.vice.com/read/v-for-vkontakte

Kaplan, Marcia (2014), "Ecommerce in Russia: Another Emerging Market?",*Practical Ecommerce*, November 12, 2014, [Online: Web] accessed. URL: http://www.practicalecommerce.com/articles/75665-Ecommerce-in-Russia-Another-Emerging-Market

Roth, Andrew and David M. Herszenhorn (2014), "Facebook Page Goes Dark, Angering Russia Dissidents", *The New York Times*, December 22, 2014, [Online: Web] accessed. URL: http://www.nytimes.com/2014/12/23/world/europe/facebook-angers-russian-opposition-by-blocking-protest-page.html?_r=0

LiveJournal (2013), "Frequently Asked Question #4. How did LiveJournal get started? Who runs it now?", [Online: Web] accessed. URL: http://www.livejournal.com/support/faq/4.html

Rigby, Sophie (2014), "Forbes Ranks the Top-10 Russian Internet Companies", *RusBase.com*, March 7, 2014, [Online: Web] accessed. URL: http://rusbase.com/news/author/sophierigby/Forbes-top10-2014/

Ries, Brian (2014), "Founder of 'Russia's Facebook' Says Government Demanded Ukraine Protestor's Data", *Mashable*, April 17, 2014, [Online: Web] accessed. URL: http://mashable.com/2014/04/16/vkontakte-founder-fsb-euromaidan/

Tam, Donna (2012), “From Facebook With Love: Zuckerberg heads to Russia”, *CNET*, September 26, 2012, [Online: Web] accessed. URL: http://www.cnet.com/news/from-facebook-with-love-zuckerberg-heads-to-russia/

Topol. Sarah A. (2014), “From Russia with Code: The Next Generation of Cyber Crime”, *Playboy*, April 28, 2014, [Online: Web] accessed. URL: http://playboysfw.kinja.com/from-russia-with-code-the-next-generation-of-cyber-cri-1568835021

The Moscow Times (2011), “Hacker Attacks Paralyze LiveJournal”, July 28, 2011, [Online: Web] accessed. URL: http://www.themoscowtimes.com/news/article/hacker-attacks-paralyze-livejournal/441237.html

Melekhov, Anton (2013), “How Russian users consume Internet (2012-2013)”, *Digital East Factor*, November 25, 2013, [Online: Web] accessed. URL: http://www.digitaleastfactor.com/how-russian-users-consume-internet-2012-2013/

Associate Press (2015), “Hundreds of thousands in Russia protest Charlie Hebdo”, *Mashable*, January 19, 2015, [Online: Web] accessed. URL: http://mashable.com/2015/01/19/charlie-hebdo-protest-russia/

Carbonnel, Alissa De (2011), “Insight: Social media makes anti-Putin protests “snowball””, *Reuters*, December 7, 2011, [Online: Web] accessed. URL: http://www.reuters.com/article/2011/12/07/us-russia-protests-socialmedia-idUSTRE7B60R720111207

East-West Digital News (2015), “The Domestic Market: Executive Summary, Part-1 of ‘E-Commerce in Russia Report’”, January 2015, [Online: Web] accessed. URL: http://.ewdn.com/e-commwwwerce/insights.pdf

Greenall. Robert (2012), “LiveJournal: Russia’s unlikely internet giant”, *BBC News*, March 2, 2012, [Online: Web] accessed. URL: http://www.bbc.com/news/magazine-17177053

IBN Live (2014), “Mail.Ru takes over ‘Russia’s Facebook’ Vkontakte”, September 17, 2014, [Online: Web] accessed. URL: http://ibnlive.in.com/news/mailru-takes-over-russias-facebook-vkontakte/499699-11.html

Center for Strategic and International Studies and McAfee Inc.(2014), “Net Losses: Estimating the Global Cost of Cybercrime: Economic impact of cybercrime II”, McAfee Inc. , June 2014, [Online: Web] accessed. URL:

Elder, Miriam (2011), “Medvedev ‘tweet’ sends the Russian blogosphere into a frenzy”, *The Guardian*, December 7, 2011, [Online: Web] accessed. URL: http://www.theguardian.com/world/2011/dec/07/medvedev-tweet-russian-blogosphere-frenzy

Essers, Loek (2014), “Music piracy battle erupts in Russia as major labels sue large social network”, *Computerworld*, April 4, 2014, [Online: Web] accessed. URL: http://www.computerworld.com.au/article/542076/music_piracy_battle_erupts_russia_major_labels_sue_large_social_network/

Holdsworth, Nick (2013), “New Anti-Piracy Law Allows Russian Rights Owners to Tackle illegal Internet Download Sites”, *Hollywood Reporter*, August 1, 2013, [Online: Web] accessed. URL: http://www.hollywoodreporter.com/news/new-anti-piracy-law-allows-597962

Hermans, Steven (2012), “New Yandex browser escalates Russia’s search-engine wars”, *Net Prophet*, October 10, 2012, [Online: Web] accessed. URL: http://netprophet.tol.org/2012/10/10/new-yandex-browser-escalates-russias-search-engine-wars/

Lunde, Ingrid (2013), “Nine Music Labels Plan To Sue Vkontakte, The Facebook of Russia, Over 6000 Illegal Tracks”, *TechCrunch*, December 27, 2013, [Online: Web] accessed. URL: http://techcrunch.com/2013/12/27/nine-big-music-labels-plan-to-sue-vkontakte-the-facebook-of-russia-over-6000-illegal-music-tracks/

Paganini, Pierluigi (2014), “Pricing Policies in the Cyber Criminal Underground”, *InfoSec Institute*, [Online: Web] accessed. URL: http://resources.infosecinstitute.com/pricing-policies-cyber-criminal-underground/

Masnick, Mike (2006), “Record Labels Finally Sue Allofmp3.com”, *Techdirt*, December 20, 2006, [Online: Web] accessed. URL: https://www.techdirt.com/articles/20061220/200724.shtml

Noyes, Katherine (2014), “Record Labels Slam Russian Social Net with Piracy”, *E-Commerce Times*, April 4, 2014, [Online: Web] accessed. URL: http://www.ecommercetimes.com/story/80247.html

Global Voices (2015), “Russia Invesitgates User for Posting Ukraine-Related Content”, January 9, 2015, [Online: Web] accessed. URL: http://globalvoicesonline.org/2015/01/09/russia-vkontakte-censorship-ukraine/

The Moscow Times (2015), “Russia Looks to Squeeze More Tax From Google-Report”, March 8, 2015, [Online: Web] accessed. URL: http://www.themoscowtimes.com/business/article/russia-looks-to-squeeze-more-tax-from-google-report/517142.html

Razumovskaya, Olga and Sam Schechner (2015), “Russia Says Twitter Not Complying with Requests for User Info”, *Wall Street Journal*, February 10, 2015, [Online: Web] accessed. URL: http://blogs.wsj.com/digits/2015/02/10/russia-says-twitter-not-complying-with-requests-for-user-info/

Investor’s Business Daily (2013), “Russia Search Engine Yandex Gets Stock Market Results”, *NASDAQ.com*, October 21, 2013, [Online: Web] accessed. URL: http://www.nasdaq.com/article/russia-search-engine-yandex-gets-stock-market-results-cm289628

Sawers, Paul (2015), “Russia takes ‘guidance’ from the E.U. in its battle with U.S. tech firms”, *VentureBeat*, March 6, 2015, [Online: Web] accessed. URL: http://venturebeat.com/2015/03/06/russia-takes-guidance-from-the-e-u-in-its-battle-with-u-s-tech-firms/

The Moscow News (2012), “Russia’s Internet use surges”, April18, 2012, [Online: Web] accessed. URL:

Reuters (2007), “Russia court acquits music site owner”, August 15, 2007, [Online: Web] accessed. URL: http://www.reuters.com/article/2007/08/15/us-russia-website-idUSL1585563020070815

Spinella, Peter (2015), “Russian Culture Ministry Keen to Tax Internet Users”, *The Moscow Times*, February 24, 2015, [Online: Web] accessed. URL: http://www.themoscowtimes.com/news/article/russian-culture-ministry-keen-to-tax-internet-users/516457.html

Kirk, Jeremy (2014), “Russian cybercrime group compromised half a million computers”, *PC World*, October 7, 2014, [Online: Web] accessed. URL: http://www.pcworld.com/article/2730352/russian-cybercrime-group-compromised-half-a-million-computers.html

Crampton, Thomas (2006), “Russian Download Site is Popular and Possibly Illegal”, *The New York Times*, June 1, 2006, [Online: Web] accessed. URL: http://www.nytimes.com/2006/06/01/world/europe/01cnd-mp3.html?_r=0

Mirovalev, Mansur and Colin Freeman (2014), “Russian hacker wanted by US hailed as hero at home”, *The Telegraph*, June 7, 2014, [Online: Web] accessed. URL:

http://www.telegraph.co.uk/news/worldnews/europe/russia/10883333/Russian-hacker-wanted-by-US-hailed-as-hero-at-home.html

Pravda.ru (2008), “Russian officials finally define pornography and ban it online”, February 26, 2008, [Online: Web] accessed. URL: http://english.pravda.ru/russia/kremlin/26-02-2008/104231-pornography-0/

Leyden, John (2011), “Russian Pres fumes at mystery DDoS hack”, *The Register*, April 8, 2011, [Online: Web] accessed. URL: http://www.theregister.co.uk/2011/04/08/russian_ddos_assaults/

Balmforth, Tom (2011), “Russian Protesters Mobilize Via Social Networks, As Key Opposition Leaders Jailed”, Radio Free Europe, December 8, 2011, [Online: Web] accessed. URL: http://www.rferl.org/content/russian_protesters_mobilize_online_as_leaders_jailed/24414881.html

Vovchuk, Vladi (2014), “Russian Shoppers Stomp on American Flag in Protest”, *Vocativ.com,* December 24, 2014, [Online: Web] accessed. URL: http://www.vocativ.com/world/russia/american-doormats-decorating-moscow-mall/

Sheremeta, Bozhena (2015), “Russia’s largest social network experiences serious technical problems”, *Kyiv Post*, January 25, 2015, [Online: Web] accessed. URL: http://www.kyivpost.com/content/russia-and-former-soviet-union/russian-largest-social-network-vkontakte-is-down-378319.html

Toor, Amar (2014), “Russia’s largest social network is under the control of Putin’s allies, founder says”, *The Verge*, April 22, 2014, [Online: Web] accessed. URL: http://www.theverge.com/2014/4/22/5638980/russias-largest-social-network-is-under-the-control-of-putins-allies

Zaks, Dmitry (2015), “Russia’s Yandex files antitrust complaint against Google”, *Business Insider*, February 18, 2015, [Online: Web] accessed. URL:

http://www.businessinsider.com/afp-russias-yandex-files-antitrust-complaint-against-google-2015-2?IR=T

Walker, Shaun (2015), "Salutin' Putin: inside a Russian troll house", *The Guardian*, April 2, 2015, [Online: Web] accessed. URL: http://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house

Six Apart (2007), "Six Apart Announces New Home for LiveJournal", December 3, 2007, [Online: Web] accessed. URL: http://www.marketwired.com/press-release/six-apart-announces-new-home-for-livejournal-798504.htm

Plesser, Ben (2014), "Skilled, Cheap Russian Hackers Power American Cybercrime", *NBC News.com*, February 6, 2014, [Online: Web] accessed. URL: http://www.nbcnews.com/news/world/skilled-cheap-russian-hackers-power-american-cybercrime-n22371

Mennecke, Thomas (2006), "AllofMp3.com Breaks Silence", *Slyck News*, June 6, 2006, [Online: Web] accessed. URL: http://www.slyck.com/news.php?story=1212

Global Voices (2015), "Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign", April 2, 2015, [Online: Web] accessed. URL: https://globalvoicesonline.org/2015/04/02/analyzing-kremlin-twitter-bots/#

Kim, Daria (2012), "Special Report Russia's Enforcement Against Online Copyright Infringement", *Intellectual Property Watch*, December 3, 2012, [Online: Web] accessed. URL: http://www.ip-watch.org/2012/12/03/special-report-on-russia-enforcement-against-online-copyright-infringement/

Baird, Dugald (2015), "Spotify abandons Russian launch plan", *The Guardian*, February 3, 2015, [Online: Web] accessed. URL: http://www.theguardian.com/media/2015/feb/03/spotify-abandons-russian-launch-plan

Shabelnikova, Alla (2014), “Spotify is coming to Russia this fall, is this the end of Vkontakte’s illegal music circulation?”,*Internet of Things News*, April 1, 2014, [Online: Web] accessed. URL: http://iotworldnews.com/2014/04/spotify-is-coming-to-russia-this-fall-is-this-the-end-of-vkontaktes-illegal-music-circulation/

Recording Industry Association of America (2011), “RIAA Highlights Russian Service Vkontakte, Others in Report to U.S. Government About Markets Rife with Music Theft”, October 26, 2011, [Online: Web] accessed. URL: https://www.riaa.com/newsitem.php?content_selector=newsandviews&news_month_filter=10&news_year_filter=2011&id=B966B360-22F9-C11E-B7A3-50777A8122E7

Hayes, Adam (2015), “Spotify Makes Internet Music Make Money”, *Investopedia*, [Online: Web] accessed. URL: http://www.investopedia.com/articles/investing/120314/spotify-makes-internet-music-make-money.asp

Gavet, Maelle (2014), “The CEO of Ozon on Building an e-Commerce Giant in a Cash-Only Economy”, *Harvard Business Review*, July 2014, [Online: Web] accessed. URL: https://hbr.org/2014/07/the-ceo-of-ozon-on-building-an-e-commerce-giant-in-a-cash-only-economy

Millar, Paula (2010), “Beware of the Spinternet”, *The Evolution of Revolution*, March 10, 2010, [Online: Web] accessed. URL: https://theevolutionofrevolution.wordpress.com/page/2/

The Economist (2012), “The Internet Business in Russia: Europe’s great exception”, May 19, 2012, [Online: Web] accessed. URL: http://www.economist.com/node/21555560

Davidoff, Victor (2011), “Web Will Win in Cyber War”, *The Moscow Times*, August 1, 2011, [Online: Web] accessed. URL: http://www.themoscowtimes.com/article.php?id=441377

Benyumov, Konstantin (2014), “The Russian Internet comes of age”, *Russia Beyond the Headlines*, July 2, 2014, [Online: Web] accessed. URL: http://rbth.com/science_and_tech/2014/07/02/the_russian_internet_comes_of_age_37887.html

Amroon, Nadia (2014), “The US Deems VK to be a Pirate Site”, RusBase.com, February 13, 2014, [Online: Web] accessed. URL: http://rusbase.com/news/author/nadiaamroon/us-deems-vk-pirate-site/

Sadchikov, Yakov (2012), “Top 10 Russian Internet Companies in 2012”, *The Moscow Times*, December 21, 2012, [Online: Web] accessed. URL: http://www.themoscowtimes.com/business/article/top-10-russian-internet-companies-in-2012/473427.html

Moyer, Edward (2012), “U.S., Russia agree on ‘action plan’ to fight piracy”, *CNET*, December 22, 2012, [Online: Web] accessed. URL: http://www.cnet.com/news/u-s-russia-agree-on-action-plan-to-fight-piracy/

The Guardian (2015), “US offers highest-ever cybercrime reward for arrest of Russian hacker”, February 24, 2015, [Online: Web] accessed. URL: http://www.theguardian.com/us-news/2015/feb/24/us-highest-ever-cybercrime-reward-evgeniy-bogachev

Out-Law.Com (2006), “US record labels file suit against Allofmp3.com”, *The Register*, December 21, 2006, [Online: Web] accessed. URL: http://www.theregister.co.uk/2006/12/21/us_labels_sue_allofmp3/

Taub, Amanda (2015), “Vladimir Putin is back. What we know about the Russian president’s “reappearance””, Vox, March 16, 2015, [Online: Web] accessed. URL: http://www.vox.com/2015/3/13/8212313/putin-missing

Morgan, Gareth (2014), “What is VK? Your guide to Russia’s largest social network”, *Marketing Tech News*, April 23, 2014, [Online: Web] accessed. URL:

http://www.marketingtechnews.net/news/2014/apr/23/what-is-vk-your-guide-to-russias-largest-social-network/

Quora.com (2013), “Who are the most famous Russian bloggers?”, March 12, 2013, [Online: Web] accessed. URL: http://www.quora.com/Who-are-the-most-famous-Russian-bloggers

Kovalev, Alexey (2011), “Why is LiveJournal still massive in Russia?”,*Wired*, February 5, 2011, [Online: Web] accessed. URL: http://www.wired.co.uk/news/archive/2011-02/04/livejournal-in-russia

Bizeul, David (2007), “Russian Business Network Study”, November 20, 2007, [Online: Web] accessed. URL: http://www.bizeul.org/files/RBN_study.pdf

Gesenhues, Amy (2014), “Yandex Reports 62 % Share of Russian Search Market with Q1 2014 Revenue up 36 %”, *Search Engine Land*, April 24, 2014, [Online: Web] accessed. URL: http://searchengineland.com/yandex-reports-36-growth-q1-2014-now-owns-62-share-russian-search-market-189860

Dillow, Clay (2013), “Yandex searches past its language barrier”, *Fortune.com*, November 13, 2013, [Online: Web] accessed. URL: http://fortune.com/2013/11/13/yandex-searches-past-its-language-barrier/

East-West Digital News (2011), “Yandex vs. Google:Why the US giant failed to conquer Russia”, May 19, 2011, [Online: Web] accessed. URL: http://www.ewdn.com/2011/05/19/yandex-vs-google-why-the-us-giant-failed-to-conquer-russia/

Cavelty, Myriam Dunn; Victor Mauer& Sai Felicia Krishna-Hensel (2007), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, England: Ashgate Publishing Limited.

Cahir, John (2004), “The Withering Away of Property: The Rise of the Internet Information Commons”, *Oxford Journal of Legal Studies*, 24 (4): 619-641.

Calista, Donald J. and James Melitski (2007), “E-Government And E-Governance: Converging Constructs of Public Sector information and Communications Technologies”, *Public Administration Quarterly*, 31(1/2): 87-120.

Dyson, Esther ; George Gilder ; George Keyworth and Alvin Toffler (1994), “Cyberspace and the American Dream: A Magna Carta for the Knowledge Age” , *Future Insight*, Release 1.2, August 1994, [Online: Web] Accessed, URL: http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html.

Deibert, Ronald J. & Masashi Crete Nishihata (2012), “Global Governance and the spread of Cyberspace Controls”, *Global Governance,* 18 (2012): 339-361.

*EFA (2002),*Internet Censorship: Law & policy around the world*, [Online: Web] Accessed, URL: https://www.efa.org.au/Issues/Censor/cens3.html.

Everard,Jerry (2000), *Virtual States: The Internet and the boundaries of the nation-state*, London: Routledge.

***** Electronic Frontier Foundation, Annual Report 2008-09

El-Nawawy, Mohammed and Sahar Khamis (2009), *Islam Dot Com: Contemporary Islamic Discourses in Cyberspace*, New York: Palgrave.

EPW (2005), “Regulating Cyberspace”, *Economic and Political Weekly*, 40 (49), pp. 5136-5137.

Franda, Marcus (2001), *Launching into Cyberspace: Internet Development and Politics in Five World Regions*, Colorado, USA: Lynne Rienner Publisher Inc.

Froomkin, A. Michael (2003), “Habermas@Discourse. Net: Toward a Critical Theory of Cyberspace”, *Harvard Law Review*, 116 (3): 749-873.

Gee, James Paul (1999), “An Introduction to Discourse Analysis: Theory and Method”, London: Routledge.

Hunter, Dan (2003), “Cyberspace as Place and the Tragedy of the Digital Anticommons” *California Law Review*, 91 (2): 439-519.

Hurwitz, Roger (1999), “Who Needs Politics? Who Needs People? The Ironies of Democracy in Cyberspace”, *Contemporary Sociology*, 28 (6): 655-661.

Jones, Reilly (1996), “A Critique of Barlow’s “A Declaration of the Independence of Cyberspace”, 8 (2), [Online: Web] Accessed, URL: http://home.comcast.net/~reillyjones/critique.html.

Jalil, KhaizuranAbd (2010), “Breaking Hegemonic dominance of the Mass Media: The Rise of Social Media”, *Department of Communication International Islamic University Malaysia*, Kuala Lumpur, Malaysia, Paper Prepared for International Conference on Communication and Media 2010 (i.COME '10), 18–20 June 2010.

Jordan, Tim (1999), *Cyberpower: The culture and politics of cyberspace and the Internet*, London: Routledge.

Johnson, David R. and David Post (1996), “Law and Borders: The Rise of Law in Cyberspace”, *Stanford Law Review*, 48 (5): 1367-1402.

Kennedy, Tracy; Barry Wellman and Kristine Klement (2003), “Gendering the Digital Divide, *IT&SOCIETY*, 1 (5): 72-96.

Keating, Lucy (2011), “UK’s top spies approved export of surveillance technology to Iran”, November 30, 2011, [Online: Web] Accessed, URL:

http://www.thebureauinvestigates.com/2011/11/30/uks-top-spies-approved-export-of-surveillance-technology-to-iran/.

Kobrin, Stephen J. (2001), “Territoriality and the Governance of Cyberspace”, *Journal of International Business Studies*, 32 (4): 687-704.

Katyal, Neal Kumar (Apr., 2001), “Criminal Law in Cyberspace”, *University of Pennsylvania Law Review*, 149 (4): 1003-1114.

Katsh, M. Ethan (1995), *Law in a Digital World*, New York: Oxford University Press.

Kluver, Randolph (2005), “The Architecture of Control: A Chinese Strategy for e-Governance”, *Journal of Public Policy*, 25 (1): 75-97.

Louise J. & Marianne W.Jorgensen (2002), *Discourse Analysis as Theory and Method*, London: *Sage Publications*.

Lessig, Lawrence (1998), “The Laws of Cyberspace”, Draft 3 1998, Essay Presented in Conference in Taipei, Taiwan, [Online: Web] Accessed, URL: https://cyber.law.harvard.edu/works/lessig/laws_cyberspace.pdf.

Lucas, Adam (1996), “Indigenous People in Cyberspace”, *Leonardo*, 29 (2): 101-108.

Loader, Brian D. (1998), *Cyberspace Divide Equality, agency and policy in the information society*, London: Routledge.

Loader, Brian D. (1997), *The Governance of Cyberspace Politics, technology and global restructuring* , London: Routledge.

Laclau and Mouffe’s Discourse Theory and Fairclough’s Critical Discourse Analysis: An Introduction and Comparison By David Rear School of Arts and Sciences Shibaura Institute of Technology ,drear@sic.shibaura-it.ac.jp

Mossberger, Karen; Caroline J. Tolbert; Hamilton, Allison (2012), “Measuring Digital Citizenship: Mobile Access and Broadband”, *International Journal of Communication,* 6 (2012): 2492–2528.

Michael L. Best and Keegan W. Wade (2009), “The Internet and Democracy: Global Catalyst or Democratic Dud?”,*Bulletin of Science Technology & Society,* 29 (4):255-271.

Morozov, Evgeny (2011), “The Net Delusion: The Dark Side of Internet Freedom”, New York: PublicAffairs™.

Mc Henry, William &ArtemBorisov (2006), “E-Government and Democracy in Russia”, *Communications of the Association for Information Systems* 17 (2006): 1064-1123,[Online: Web] Accessed, URL: http://aisel.aisnet.org/cais/vol17/iss1/48/.

Maloney, Marilyn C. (1997), “Intellectual Property in Cyberspace”, *TheBusiness Lawyer,* 53 (1): 225-249.

Mueller, Milton L. (2002), *Ruling the Root: Internet Governance and the Taming of Cyberspace,* London: The MIT Press.

Morozov, Evgeny (2009), “Censoring cyberspace”, *RSA Journal*, 155 (5539): 20-23.

Netanel, Neil W. (2000), “Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory”,*California Law Review,* 88 (2): 395- 498.

New Media Trend Watch, COUNTRY PROFILE- Russia, [Online: Web] Accessed, URL: http://www.newmediatrendwatch.com/markets-by-country/10-europe/81-russia?showall=1

Open Net Initiative (2010), “Country Profile of Internet Filtering: Russia”, [Online: Web] Accessed, URL: https://opennet.net/sites/opennet.net/files/ONI_Russia_2010.pdf

Perritt, Henry H. Jr. (1998), “The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in StrengtheningNational and Global Governance”, *Indiana Journal of Global Legal Studies*, 5 (2): 423-442.

Portnoy,Michael & Seymour Goodman (eds.) (2009*), Global Initiatives to Secure Cyberspace: An Emerging Landscape,* New York: Springer Science+Business Media, LLC.

Polat,RabiaKarakaya (2005), “The Internet and Political Participation: Exploring the Explanatory Links”, *European Journal of Communication,* 20 (4): 435- 459.

Ryan, Johnny (2010), *A History of the Internet and the Digital Future*, London: reaktion books ltd.

Russia- Open Net Initiative, [Online: Web] Accessed, URL: https://opennet.net/sites/opennet.net/files/ONI_Russia_2010.pdf

Rose, Richard (2005), “A Global Diffusion Model of e-Governance” *Journal of Public Policy*, 25 (1): 5-27.

Russell, Gabrielle (2008), “Pedophiles in Wonderland: Censoring the Sinful in Cyberspace”, *The Journal of Criminal Law and Criminology,* 98(40): 1467-1500.

Rosenzweig, Sidney A. (1995), "Don't Put My Article Online!: Extending Copyright's New-Use Doctrine to the Electronic Publishing Media and beyond", *University of Pennsylvania Law Review*, 143(3): 899-932.

Starrs, Paul F. (1997), "The Sacred, the Regional, and the Digital", *Geographical Review*, 87 (2): 193-218.

Steinberg, Philip E. and Stephen D. McDowell (2003), "Global Communication and the Post-Statism of Cyberspace: A Spatial Constructivist View", *Review of International Political Economy*, 10 (2): 196-221.

Smith, Marc A. and Peter Kollock (1999), *Communities in Cyberspace*, London: Routledge.

Sylvester,Dari E.and Adam J. McGlynn, (2010), "The Digital Divide, Political Participation, and Place", *Social Science Computer Review* 28 (1): 64- 74.

Sassen, Saskia (2002), "Mediating Practices: Women With/in Cyberspace" in John Armitage and Joanne Roberts (eds.) *Living with Cyberspace: Technology & Society in the 21st Century*, Continuum: London.

Stehn, Jurgen (2003), "International Trade in Cyberspace: How to Tax Digital Goods", *Journal of Economic Integration*, 18 (2): 243-265.

The SecDev Group (2012), "Neither Here Nor There: Turkmenistan's Digital Doldrum", October 2012, [Online: Web] Accessed, URL: http://www.opensocietyfoundations.org/sites/default/files/neither-here-nor-there-20130116.pdf.pdf

Warf, Barney and Grimes John (1997), "Counter hegemonic Discourses and the Internet", *Geographical Review*, 87 (2): 259-274.

Wilson III, Ernest J. (2005), "What Is Internet Governance and Where Does It Come From?",*Journal of Public Policy*, 25 (1): 29-50.

Warf, Barney and Peter Vincent (2007), "Multiple Geographies of the Arab Internet" *Area*, 39 (1): 83-96.

Winner, Langdon (1997), "Technology Today: Utopia or Dystopia?",*Social Research*, 64 (3): 989-1017.

Wilhelm, Anthony G. (2000), *Democracy in the Digital Age Challenges to Political Life In Cyberspace*, New York: Routledge.

Wagner, Abraham R. (2005), "Terrorism and the Internet: Use and Abuse", in Mark Last & Abraham Kandel (eds.), *Fighting Terror in Cyberspace*, Singapore: World Scientific Publishing Co. Pvt. Ltd.

Wagner,Ben (2012), "Exporting Censorship and Surveillance Technology", Humanist Institute for Co-operation with Developing Countries (Hivos), [Online: Web] Accessed, URL: https://www.google.co.in/webhp?source=search_app&gws_rd=cr&ei=PfA6UurdBonyrQfI7ICoBQ#q=EXPORTING+CENSORSHIP+AND+SURVEILLANCE+TECHNOLOGY+by+Ben+Wagner.

Zaharchenko, Tatiana R. (2009), "On the Way to Transparency: A Comparative Study on Post-Soviet States and the Aarhus Convention", Occasional Paper #303,2009, Woodrow Wilson International Center for Scholars, [Online: Web] Accessed, URL: http://www.wilsoncenter.org/sites/default/files/op303_on_way_to_transparency_zaharchenk_2009.pdf.

Watkins, Tom (2014), “Snowden questions Putin on camera”, *CNN*, April 18, 2014, [Online: Web] accessed. URL: http://edition.cnn.com/2014/04/17/world/europe/russia-snowden-putin/

Soldatov, Andrei and Irina Borogan (2013), “Russia’s Surveillance State”, *World Policy Journal*, 30 (3), Fall Issue, [Online: Web] accessed. URL: http://www.worldpolicy.org/journal/fall2013/Russia-surveillance

Tracy, Jen (2000), “Police Get Window of Access to E-mail”, *The Moscow Times*, January 13, 2000, [Online: Web] accessed. URL: http://www.themoscowtimes.com/sitemap/free/2000/1/article/police-get-window-of-access-to-e-mail/268089.html

*Federal Service for Supervision of Communications Information Technology and Mass Media , Russian Federation (2015), “Roscomnadzor’s Priority Objectives Identified by its Head A. Zharov”, April 20, 2015, [Online: Web] accessed. URL: http://eng.rkn.gov.ru/news/news51.htm

Razumovskaya, Olga (2015), “Russia and China Pledge Not to Hack Each Other”, *Wall Street Journal*, May 8, 2015, [Online: Web] accessed. URL: http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/

Bernstein, Leandra (2015), “Ex-US Intelligence Officer Worries About Russia-China Cyber Security Pact”, Sputnik News, May 12, 2015, [Online: Web] accessed. URL: http://sputniknews.com/military/20150512/1022061006.html

Peters, Sara (2015), “What Does China-Russia ‘No Hack’ Pact Mean For US?”,*Dark Reading*, May 11, 2015, [Online: Web] accessed. URL: http://www.darkreading.com/vulnerabilities---threats/advanced-threats/what-does-china-russia-no-hack-pact-mean-for-us-/d/d-id/1320365

Chernenko, Elena, et al (2014), “China and Russia Forge Cybersecurity Partnership Without the U.S.”, *Worldcrunch*, October 30, 2014, [Online: Web] accessed. URL: http://www.huffingtonpost.com/worldcrunch/why-russia-and-china-see-_b_6071528.html?ir=India&adsSiteOverride=in

Jiao, Wu and Zhao Shengnan (2014), “Xi: Respect cyber sovereignty”, *China Daily*, July 17, 2014, [Online: Web] accessed. URL: http://usa.chinadaily.com.cn/epaper/2014-07/17/content_17818027.htm