DIGITALISATION AS EXCLUSION: ENVISAGING EMANCIPATION IN CYBERSPACE

Dissertation submitted to Jawaharlal Nehru University
in partial fulfilment of the requirements
for award of the degree of
MASTER OF PHILOSOPHY

STANZIN LHASKYABS

Diplomacy and Disarmament Division
Centre for International Politics, Organisation and Disarmament
School of International Studies
JAWAHARLAL NEHRU UNIVERSITY
New Delhi 110067
2016

Centre for International Politics, Organization and Disarmament
School of International Studies
JAWAHARLAL NEHRU UNIVERSITY
New Delhi - 110067, India

Date:

DECLARATION

I declare that the dissertation entitled **"DIGITALISATION AS EXCLUSION: ENVISAGING EMANCIPATION IN CYBERSPACE"** submitted by me for the award of the degree of **Master of Philosophy** of Jawaharlal Nehru University is my own work. The dissertation has not been submitted for any other degree of this University or any other university.

STANZIN LHASKYABS

CERTIFICATE

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

PROF. C. S. R. MURTHY

Chairperson, CIPOD

Chairperson
Centre for International Politics,
Organization and Disarmament
School of International Studies
Jawaharlal Nehru University
New Delhi-110067

JMadhan Mohan

DR. J. MADHAN MOHAN

Supervisor

Centre for International Politics,
Organization and Disarmament
School of International Studies
Jawaharlal Nehru University
New Delhi-110067

ACKNOWLEDGEMENT

Writing this dissertation journey was indeed a great experience of learning, unlearning, and emancipation. I am indebted to my supervisor Dr. J. Madhan Mohan for showing me the light in the path of this challenging journey. The light always motivated and pushed me beyond the boundaries of my capability and reach. Had it not been him, this piece of work would not have been possible. Also, I would like to thank the faculty members and the staff of school for their support.

A note of thank you also goes to all my classmates of diplomacy and disarmament division. They always have been my inspiration right from the day one. Their brilliance in research and domain knowledge always captured my imaginations. Apart from the studies they have always been supportive and helpful.

Lastly, I would like to thank my friends and research buddies, especially Tanushree, Shayesta, Manu, Anu, and CKB, for their timeless support.

CONTENTS

ABBREVIATIONS

IR	International Relations
UIAD	Unique Identification Authority of India
RMA	Revolution in Military Affairs
MIT	Massachusetts Institute of Technology
GOP	Guardians of Peace
USA	United States of America
NCCCIC	National Cybersecurity and Communications Integration Center
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command
DOD	Department of Defence
ICT	Information, Technology & Communication
LGBTI	Lesbian Gay, Bisexual, Transgender and Intersex
LCD	Least Developed Countries
TRAI	Telecom Regulatory Authority of India
UAE	ıited Arab Emirates

LIST OF TABELS AND FIGURES

Chapter 1

INTRODUCTION

With the recent growth of digitalisation across the world, there is no doubt that the domain of cyberspace is increasing at a rapid rate. It is ready to consume and include anything and everything that is left undigitalised. As evident from the recent developments in world affairs, even the discourse of International Relations (IR) is incomplete without bringing the context of cyberspace. Cyberspace is known as a virtual space created by networks of information technology devices which involve computers used at the three levels: individual, state and international system. This virtual space is a largely contested subject among the scholars where the rhetoric of its advantages in terms of bringing development and progressive change in international society largely dominates. However, there is limited scholarly attempt to understand what this progressive change means for the marginalised sections of international society. More acutely, in the realm of IR there has always been a lack of genuine attention towards the voices of the marginalised and minorities. This is prevalent both in theory as well as practice. While we delve into the discourse of cyberspace in IR, there is a major gap to understand and hear the unheard voices in international society. Therefore, this study aims to address the relevance of the uncritical expansion and 'securitisation' of this 'space' to the marginalised sections of the international society. In other words, the study is an attempt to emancipate the discourse of cyberspace.

> Moving away from emphasising only on theoretical deliberations it is equally essential to examine the subject from 'critical problem solving approach' and address the real problems faced by the marginalised (Brown 2013).

Concerns of marginalised and the wretched (Brown 2013) have always been sidelined and remained on the fringes of mainstream IR. This serves the interests of the privileged few: capitalists and the state. A similar trend can be seen in the domain of cyberspace as well.

The key claim for the fast rapid expansion of cyberspace, mainly propagated by states and private players, is the argument of inclusion of everyone in society for development and progressive change. Many developing states like India, China and Africa are already propagating this logic to digitise every individual. For instance, India has started making one of the world's largest databases of its citisen by creating Unique Identification Authority of India (UIAD) in 2009. It has also recently launched the ambitious 'Digital India Programme' which speaks of the vision of transforming India into 'digitally empowered society and knowledge society'. However, the question is: are the marginalised Indians going to get substantial benefits out of these schemes? What does 'digital empowerment' mean to the poor Indians who lack basic facilities such as toilets, electricity and home? Can we consider basic internet, as claimed by Facebook, as a basic need to them? How relevant is this knowledge society to the tribal societies of India whose knowledge is more sustainable and friendly to nature than the knowledge produced by industrialisation? There are many such questions which actually take to the understanding that perhaps the expansion of cyberspace actually excludes the marginalised sections of the society. In other words, it is in the interest of the *status quo* of dynamics of power that the current expansion of cyberspace is being promoted and propagated.

This interest is further controlled by securitisation of cyberspace. Cybersecurity in International Relations is largely looked as a security from the threats of cyber attacks in the form of malicious software that can harm data available in cyberspace that are critical and sensitive to a state. The greatest concern is anonymity of the attacker and the potential impact of such attacks on the physical real world, which can be detrimental to economic, political, social and ecological harmony of a state. Therefore, many states today take pre-emptive measures to secure cyberspace from such attacks. In the process, these measures end up suppressing the voice of the marginalised either by disrespecting their privacy or by snatching their basic rights of freedom of expression and representation. In this context, it is necessary to define cybersecurity in terms of emancipation.

The Welsh or Aberystwyth School of Critical Security Studies talks of emancipation which means ‘freedom of individuals from all kinds of constraints’ to carry their choice of action, which is compatible with others’ ‘freedom’ (Booth 2007). It is in this context that cybersecurity can be defined as a security of an individual, group, society, community or a state in cyberspace which is compatible to others’ (individual/group/society/community/state) freedom. That is to reiterate that the concerns and voices of the marginalised should not be compromised in the existing set-up of cyberspace.

Cyberspace

Cyberspace has caught the attention of IR scholars when more and more entities like society, institution, organisation, and state started rapidly to rely over this space for their practical processes and needs. From the Revolution in Military Affairs (RMA) into the social networking sites, it has entered into the lives of everybody that could afford to buy computers and other necessary devices. Cyberspace is the reflection of existing international system in a new domain (Liaropoulos 2013). How we perceive cyberspace and with what mindset will determine the future design of cyberspace for generations of individuals and societies (Kremera 2014). Kremera (2014) further proposes perceiving security of cyberspace from liberal-mindset. This mindset, unlike the military mindset, is based on human security conception (Kremera 2014).

The concerns of marginalised has always remained on the fringes of mainstream IR (Brown 2013). He strongly argues that there is poverty in grand theory and it is time to speak up for the marginalised and the wretched in IR discourse using critical problem solving approach. What use is theory when it is not even able to address the practical problems that are being faced by the marginalised today in the world?

On the other hand, in the beginning of 2000’s few scholars saw a new hope in this ever expanding cyberspace, which is open in nature, by stating that information technology has created a new platform for the previously marginalised non-state actors to launch their activism and awareness movements (Dartnell 2003). However, now there is growing concern that the rapid expansion of this cyberspace is primarily working in the interests of the states and private companies so that the power dynamics of the status-quo can remain undisturbed (Deibert 2003; Carr 2015).

For instance, during G8 summit in Okinawa in 2000, the prime objective of the West towards digitising Africa was not development but trade and communication which can eventually work for the interest of the West (Alden 2003). Within a state, the nexus between the state and private multi-nationals always control the flow of information through cyberspace.

Cybersecurity

Within last thirty years the nature of cyber attacks has evolved from a very elementary and inconsequential computer virus by students in computer labs to highly assaulting attacks by well organised hackers (Houser 2015). In 2010, Iranian Nuclear Facility was attacked by a Stuxnet virus, which destroyed many centrifuges used to enrich Uranium (Nye 2011). Last year in 2014 Sony, Home Depot, JP Morgan, eBay, Gmail, Mizilla, Korea Credit Bureau and many other enterprises were affected by cyberattacks (Houser, 2015). Interdependence and vulnerability (Nye 2011) are two main characteristics of cyberspace under the constant change and development of technology.

In response to such growing cyberattacks, securitisation of cyberspace began to take place. For instance, Post September 11, United State started focusing the security of cyberspace (Weber and Heinrich 2012). United States Cyber Command, National Response Center for Cyber Crimes of Pakistan, Pakistan Information Security Association, India’s National Technical Research Organisation, Information Sharing and Analysis Center, National Critical Information Infrastructure and Protection Center, and Computer Emergency Response Teams (Baker 2014) are some of the state agencies established in response to counter cyber attacks. In addition, there is growing number of states producing Cyber-policies to protect their cyber-infrastructure and control the access of information by the citizens (Liaropoulos 2013).

However, state agencies and the scholars in International Relations have predominantly understood the concept of Cybersecurity as defined by Neo-Realists. Even in the scholarly work, Cybersecurity is explained with the assumptions of clear dichotomy between ‘us’ and ‘they’, enemy and friend, and military approach of security.

Cyberwar (Libicki, 2009), cyberdeterrence (Libicki 2009), strategic cyberwar (Libicki, 2009), cybertriad (Harknett and Stever 2009) are terminologies taken from the dictionary of the Neo-Realist tradition of understanding security. There is tendency of assigning Cybersecurity as Strategic. This is however, a contested topic (Kavanagh 2014). Most of these works by the experts in IR are heavily skewed towards the interests of state and private players. That is, they would never move away from the inherent existence and selfish nature of state. The threat from cyberspace is blown out of proportion so much so that invention of cyberspace is incredibly compared with the invention of Nuclear Bomb by (Nye 2012).

Therefore, there is an attempt to understand Cybersecurity from non-traditional perspective. For instance, Hansen and Nissenbaum (2009) operationalise cybersecurity from the Copenhagen School of Security Studies.

Emancipation

Emancipation, as propounded by Ken Booth (2007), constitutes the following three strands: Philosophical anchorage of knowledge, Theory of progress for society and a Practice of resistance against oppression. It is conception of being free from all the physical and human constraints that is being propagated by the notion of emancipation.

The notion of emancipation depends on the understanding of Freedom. Ken Booth (2007) states that it is the true freedom and not the false freedom that is associated with emancipation. False freedom comes with the negative human side in the form of freedom of doing anything that cause non-violence and harm to other human beings. The true freedom is the one where the positive side of human mind is reflective. This includes the notion of freedom to execute anything which does not harm others. In emancipatory security, individual and human freedom takes precedence over state and power (Booth 1991). To elaborate further, as Ken Booth (1991) posits that individuals should be considered as end and not means. state and all other non-human related entities should consider as means to attain emancipation of individuals.

In addition, there is non-dual relationship between security and emancipation (Booth 1991). That is, security must be treated as a means to achieve emancipation, and emancipation should be used to achieve security.

Cyberspace is known as a virtual space created by networks of information technology devices which involve computers used at the three levels: individual, state and international system. It is because of the securitisation of this virtual space that the concept of Cybersecurity has emerged. Understanding Cybersecurity from the perspective of Welsh School of Critical Theory, it can be defined as the security of an individual, group, society, community or a state in cyberspace which is compatible to others' (individual/group/society/community/state) freedom. It is the freedom from constraints of all these entities which is not against or harming any other entity. It is the emancipation of every entity or sentient beings within and outside the ambit of cyberspace, especially the marginalised, that Cybersecurity is defined in this paper.

I take the notion of marginalised section as those sections of individuals, societies, communities, regions, and states which are always kept on the fringes of mainstream. For instance, minorities based on religion, sex, region, colour, language, ability, wealth, region, community, religion, etc. Therefore, the definition cuts across the firm boundaries of conventional mainstream states and encapsulates all forms and means of marginalisation.

What is puzzling is while cyberspace, which is meant for the good of all, despite growing exponentially is unable to address the concerns of the marginalised and serving the needs of privileged few. Digitisation is taking place everywhere and yet there is a sense of vacuum as far as the needs of the marginalised are concerned. For instance what does inclusion in cyberspace mean to the people of indigenous tribes of Amazon Forests? Why the internet giants like Facebook and Google filter information specific to certain countries like China and India?

Normatively, since the voice of marginalised and wretched are hardly represented in International Relations discourse, I feel the need to bring their concerns and perspectives on the table.

The perspective of the marginalised is important as it is evident from the following famous lines from Mahatma Gandhi:

> I will give you a talisman. Whenever you are in doubt, or when the self becomes too much with you, apply the following test. Recall the face of the poorest and the weakest man (woman) whom you may have seen, and ask yourself, if the step you contemplate is going to be of any use to him (her). Will he (she) gain anything by it? Will it restore him (her) to a control over his (her) own life and destiny? In other words, will it lead to *swaraj* for the hungry and spiritually starving millions? Then you will find your doubts and yourself melt away.

As far as scope is concerned the paper does not addresses the technical side of the cyberspace and Cybersecurity. Though, it is going to touch upon the technical aspects, it will not get into the details due to time and resource limitations. The marginalised sections in the paper are being discussed in general terms, therefore no specific case study is being considered.

This dissertation addresses the following key questions:

1. What does it mean to the marginalised section of the society to be a part of cyberspace?
2. Is cyberspace bringing development and change among the marginalised as claimed by others?
3. How do these inclusions on the space actually serve to the rhetoric of inclusive development?
4. Are the marginalised feeling more empowered being part of the digital world?
5. What does securitisation of cyberspace mean for the wretched, poor and underrepresented sections of the society?
6. How does the marginalised view cybersecurity?

In order to address these questions, the following hypotheses are proposed:

1. Securitisation of cyberspace results in a suppression of the voices of the un-heard in the international society
2. Inclusivity in cyberspace is leading to exclusivity of the marginalised.

These hypotheses are not mutually exclusive as they overlap each other. However, it is essential to keep these two separate as each of these addresses two critical aspects of cyberspace that affect the marginalised. The first questions the uncritical expansion of and thereby the claim of inclusiveness in cyberspace. And the second addresses how through the means of Securitisation, the few privileged suppress the voices of marginalised.

Research Method

The method of research in this paper is primarily based on qualitative analysis. The study does not restrict to the sources only to International Relations. It takes the reference from the sources that are widely grounded in the understanding of nature of the problem. That is to say that the area of the research data is not restrained by the very discipline of study. The advantage of this is that it enables the researcher to address the research problem in a holistic way. Therefore, the references are from varied disciplines like sociology, law, international relations, science and technology, philosophy and defence & strategic studies.

Largely secondary sources like reports, academic journals, periodicals, newspapers, online materials, magazines, and books are referred for the study. While the academic journals and periodicals enabled a very in depth understanding of the research area from academic point of view, the online materials, magazines, reports, and newspapers unfolded the practical view of the research problem. The sources, therefore, provided a good understanding of the area of study from both theory and practice.

Organisation of dissertation

Chapter 1: Introduction

This first chapter consists of basic introduction to the research topic including the research puzzle and the objective it tries to achieve.

Chapter 2: Securitisation of cyberspace

The second chapter covers the securitisation of the cyberspace and its impact on the marginalised by engaging in both theory and practice.

Chapter 3: Inclusion in cyberspace as mxclusion of Marginalised: A paradox of globalisation

The third chapter engages with the exclusion of marginalised. It addresses the exclusion of the marginalised sections from the larger social, political and legal ambit of the international society. Primarily the globalisation is examined here along under the context of cyberspace.

Chapter 4: Emancipation in cyberspace

The last chapter engages with the emancipatory notion of securitisation and emancipation in cyberspace.

Chapter 5: Conclusion

This chapter engages summarises the findings of the study.

Chapter 2

SECURITISATION OF CYBERSPACE

Theory of Securitisation

The Securitisation theory by Copenhagen School marked a departure from the traditional understanding and conception of security. The process of securitisation, which is elevating an issue from the 'normal politics' to 'high politics', does not necessarily reflect the objective circumstances as propounded by the realists. For Copenhagen School the securitisation is speech claim by securitisation actor about an issue which, if not dealt extraordinarily beyond the rule book, could possess existential threat to audience of securitisation (Buzan et al. 1998). In similar tone, we can understand the concept from sociological point of view as Thierry Balzacq (2011: 3) defines securitisation as:

> ...an articulated assemblage of practices whereby heuristic artefacts (metaphors, policy tools, image repertoires, analogies, stereotypes, emotions, etc.) are contextually mobilised by securitizing actor, who works to prompt an audience to build a coherent network of implications (feelings, sensations, thoughts, and institutions), about the critical vulnerability of a referent object, that occurs with the securitisation actor's reasons for choices and actions, by investing the referent subject with such an aura of unprecedented threatening complexion that a customised policy must be undertaken immediately to block its development.

With much criticism on Copenhagen school (Mclnnes and Rushton 2011), the Securitisation theory today has evolved to be one of the important discourses in the field of International Relations Theory. Consequently, the understanding of Securitisation has also evolved. Not limiting to just being 'speech act' as proposed initially by Copenhagen School, securitisation today includes all the processes of communication and actions, by a securitising actor, which shapes the perception of security among the audience.

Restriction of securitisation process merely as ‘speech act’ brings out an important challenge to Copenhagen School of Security as rise of ‘televisual’ communication used by institutions and organisation, including non-state actors, which does not necessarily utter the word ‘security’, do have role in the process of securitisation (Williams 2003).

However, much of these criticisms, with exceptions like (Hansen 2000) still distance themselves from the referent object of individual security as a part of the securitisation theory. The scathing attack that she makes on Copenhagen school is a breakthrough in securitisation theory, where she ruptures the parochial view of securitisation with society, institutions and states as only referent objects and highlights the need to count individual as a crucial referent object. Thereby raising a strong concern of security where the very ‘speech act’ is not possible or silenced. Also, in agreement with Stritazel (2007), Watson (2011) makes the point that Copenhagen School has ignored the various security activities that takes in ‘normal politics’ scenario.

Analysing process of securitisation, Mclnnes and Rushton (2011) makes three important points. First, ‘Multi-level’ securitisation process might occur from lower level to systemic level and that the role of securitising actor and audience varies at different level. Not giving importance to the role of audience is one of the crticisims of the Copenhagen School (Williams 2003). Just satisfying the three ‘facilitating conditions[1]’ as propounded by Buzan et al. (1998), does not necessarily lead to success in securitisation; the success also requires persuasion of the audience to believe that an issue is existential threat. Second, securitisation is not binary. Rather it is a continuum where what is securitsed and not securitised (normal politics), are ‘two ends of a specturm’. The third is that role of ‘empirical evidence’ do play an important part in the securitsation process – where doubt arises over the evidence there is a possiblity of desecuritsation.

[1] These conditions are: 1. the speech act must follow grammar of security, that is, it must point to existential threat 2. The speech act must be from somebody with social position so that the audience can readily accept the speech 3. Attributes of the object of threat that can either facilitate or restrain securitisation

Another critique on the Copenhagen School is its negative tone towards securitisation. For Copenhagen School ‘securitisation’ is often understood in a negative connotation as despite its criticism towards state’s security policies and strategies, it has not been able to separate themselves from statist definition of security. It has therefore, leaned in favour of desecuritsation.

To this, many have challenged and even argued that the question is not about securitisation being positive or negative. It depends on the context and the definition of the security.

For instance, Critical Security Studies or Welsh School of Security analyst defining security is primary importance while engaging with securitisation. It states that ultimate goal of security is nothing but emancipation. Emancipation, as propounded by Ken Booth (2007), constitutes the following three strands: Philosophical anchorage of knowledge, theory of progress for society and a practice of resistance against oppression. It is conception of being free from all the physical and human constraints that is being propagated by the notion of emancipation.

The notion of emancipation depends on the understanding of Freedom. Ken Booth (2007) states that it is the true freedom and not the false freedom that is associated with emancipation. False freedom comes with the negative human side in the form of freedom of doing anything that cause non-violence and harm to other human beings. The true freedom is the one where the positive side of human mind is reflective. This includes the notion of freedom to execute anything which does not harm others or does not deprive others of the same freedom. In emancipatory security, individual and human freedom takes precedence over state and power. In fact, Booth (1991) posits that individuals should be considered as end and not means. State and all other non-human related entities should consider as means to attain emancipation of individuals. In addition, there is non-dual relationship between security and emancipation (Booth, Security and Emancipation 1991). That is, security must be treated as a means to achieve emancipation, and emancipation should be used to achieve security. In this sense the Welsh school takes securitisation as a positive concept; that which should lead to emancipation of everyone at individual level.

The debate whether securitisation or desecuritsation, inherently, is positive or negative becomes irrelevant because what determines them positive or negative depends on securitisation move of the actor and securitisation practice on the audience (Diskaya 2013). What is positive is that ultimately the practice should lead to human welfare and well-being; in no case it should harm or have negative impact on individuals or limit human emancipation (Diskaya 2013).

Floyd (2007), in trying to understand both Copenhagen School and Welsh School as complimentary, defines positive and negative securitisation based on the common attribute of 'mobilisation power':

> This article has criticised Waever et al. for having too pessimistic a view of security and what it can do, whilst at the same time criticising the Welsh School for being too optimistic in their view of security. The analysis has identified the acknowledgement of the 'mobilisation power' of security as a shared assumption in both schools. From there it has proceeded to argue that this 'mobilisation power' can potentially be put to good use with securitisation as just the 'right' solution to some problems. This has been called positive securitisation. It is this concept, and only this one, upon which a normative theory of security, such as that of the Welsh School, should be built. This is so, because the 'mobilisation power' of security can be used or abused and put to limited, fake, or worse, malicious intentions resulting in what has here been called negative securitisation (Floyd 2007).

Floyd (2007) terms this analysis of securitisation as 'Consequentialist evaluation of Security'. Her analysis rightly dispels the confusion of looking securitisation as inherently negative and positive. For no concept or phenomenon can be described in an absolute terms or binary.

Considering Welsh School's definition of security and Thierry Balzacq's (2011: 3) definition, securitisation can be defined as:

A set of behaviours whereby 'heuristic artefacts' (emotions, policy, image collections, and cultural norms) are 'contextually mobilised' by the securitising actor to motivate an audience to build a common web of implications (feelings, sensations, thoughts, and institutions), about the 'critical vulnerability' of an individual, that takes place with securitising actor's reason of understanding individual as an inherent and most crucial part of the larger functional[2] systems[3] by highlighting the 'referent subject' as threat to the emancipation of individual that an immediate action plan must be taken in order to restrict its further development.

This definition, though still in tentative stage and in contrary to Copenhagen School of thought, is not to be understood that the definition disregard the Copenhagen school of Securitisation. Just that this definition tries to focus on two things: firstly, to have more positive understanding of securitisation and secondly to bring out the essence of individual in International Relations. This is because firstly having a positive understanding sets tone to an ideal definition which is crucial in terms of consequential analysis. For an ideal definition must guide the actions. Secondly, without individuals all other systems become invalid and null. However, definition captures and agrees to the existence of functional system beyond individual like family, society, community, nation, state and world, and at the same time it emphasises that individuals, the real constituents of these systems, cannot be sidelined or deprivileged before these systems.

The question is how can we juxtapose the dominant conceptualisation of securitisation, as originally propounded by Copenhagen School, with this working definition? As Floyd (2007) used the term abuse of mobilizing power, the dominant conceptualisation of securitisation can be simply summed up as exploitation of securitisation. That is, when securitisation is misused by securitising actor with malicious intent or in the interest which is against the emancipation of individuals.

Cybersecurity as Securitisation of Cyberspace

Most of the literature in International Relations has discussed securitisation of cyberspace on the basis dominant Copenhagen School of thought. Rarely there are any serious deliberations from the perspective of individual as an important and critical part of the system in general.

[2] Functional in the sense these concepts exist at the level of function. That is, their existence becomes invalid without their functions.

[3] System includes family, community, society, nation, state and world.

As discussed before, it is not to undermine the existing narratives of the securitisation school in literature as well as practice; unprivileged position of individual in the analysis of International Relations is worth a concern. In fact, visualising the system from bottom up is as crucial as it is visualising from top to bottom; perhaps, more relevant in modern times.

Traditional Securitisation of Cyberspace

Cybersecurity as a concept emerged out of changing world geopolitical conditions and advancement in technology post cold war (Hansen and Nissenbaum 2009). One of the early cyber attacks took place in 1988 when Morris Worm, created by Massachusetts Institute of Technology (MIT) professor Robert Tapan Morris, affected large computers of United States. The worm would slow down the computer to the point that it becomes unusable (NATO Review n.d.). There has been considerable change in the mode of attack on the cyber network in the last three decades. From very casual and inconsequential computer viruses by students to high impact cyber attacks by well organised hackers (Houser 2015), effecting not only individuals but also various multinational corporations and states. In 2010, the Stuxnet virus attacked centrifuges used to enrich Uranium in Iranian Nuclear Facility (Nye 2011). Many enterprises and institutions like Sony, Depot, JP Morgan, eBay, Gmail, Mozilla, Korea Credit Bureau were cyber attacked in 2015 (Houser 2015).

Table 2.1.1 shows timeline of major cyber attacks from 1998 to 2015. There is interesting trend of attacks being targeted mostly on the governments of developed states, especially United States. In 2012, the operation ‘Red October’ was identified which is an advanced cyber-espionage which had been targeting critical diplomatic and government documents of various states from the last five years. This spread of information theft was not just limited to one particular state; rather it was targeting multi-state governments, diplomats and institutions. Russian federation, Kazakhstan, Azerbaijan, Belgium, India, Afghanistan, and Armenia were most affected states. (Kaspersky Lab 2013).

The primary trigger behind these cyber attacks are claimed to be political. For instance, the massive attack on the networks of government systems of Estonia occurred after the spat between Estonia and Russia when Estonia removed the war memorials statues.

In 2014, computer network of the Sony Corporation was hacked when it came out with the controversial political satire movie ‘The Interview’. The attack was claimed to be carried out by a group called Guardians of Peace (GOP) which breached the security networks of Sony’s studio in Hollywood and compromised the information of company’s project and employees leading to the delay in movie release. The move by GOP was mainly aimed at stopping the release of the movie which shows assassination of North Korean leader Kim Jong-un (Rushe 2015). It cost Sony $15 million to repair the damage caused by the attack. Although there were no concrete evidence, United States alleged that the GOP is backed by North Korea. North Korea later clearly denied the charges against it. Later in early 2015, Obama administration imposed sanctions against North Korea in response to the alleged cyber attack effecting already tensed relation between the two countries.

The other motive behind the cyber attack is economic gains. The attackers take the advantage of highly interconnected computer networks across the world targeting individuals, banks, institutions, private and government accounts to gain monetary benefits. This is either done by directly hacking users account details or by using other indirect means.

The information that were compromised or stolen by hackers in 2015, in the figure 2.1.1, includes personal information like username, password, and birthdates, and credit-debit cards of customers which are primarily used to steal money. In fact, in its security report by CISCO (2016), making money is top agenda for the modern computer hackers. The explosion of ransomware[4] is the latest trend where extracting money becomes easy for the hackers by directly asking money from the victims. CISCO (2016) reports that gross yearly income for a ransomware called *Angler Exploit Kit* is $34 million annually where 9515 users pay ransoms per month.

The new age cyber attacks are now directly targeting financial institutions and banks. Since late 2014 the attacks have been more frequent. For instance, Bangladesh Central Bank lost more than $100 million from its account at the Federal Reserve Bank of New York in February 2016 when the hackers stole the money using complex cyber tools.

[4] *Ransomware* keep critical information of users as hostage and extract money from the victims

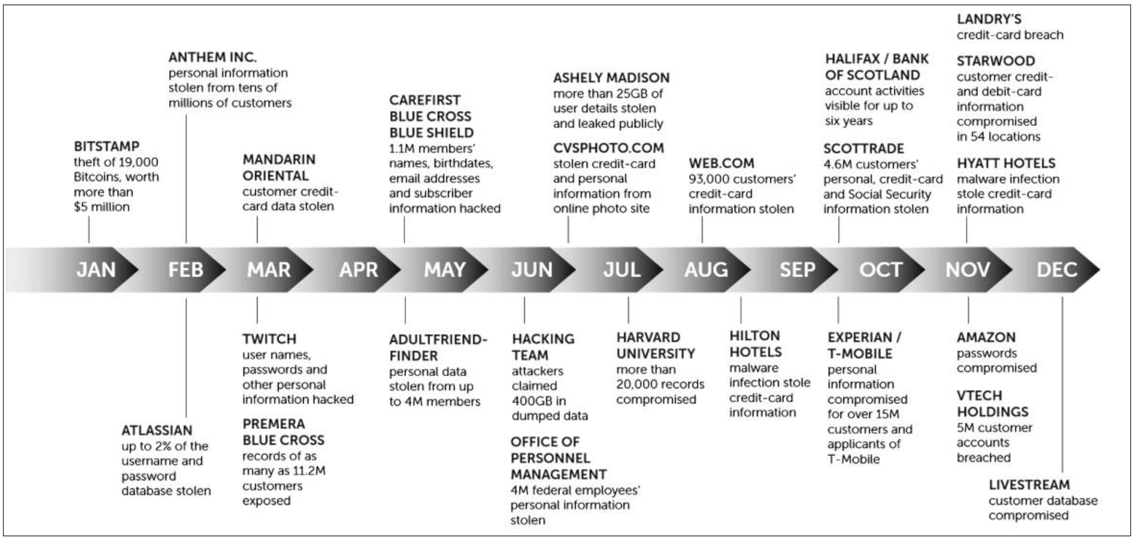
The attackers posing as officials of Bangladesh Central Bank sent e-mails to the New York Federal Bank requesting transfer of amount to accounts located in Philippines and Sir Lanka (Al-Mahmood 2016). Another recent case is a malware called *Carbanak* which is widespread in the computer systems of Russia, USA, Germany, China and other developed nations. It is estimated that *Carbanak* caused a damage of $1 billion (Kaspersky Lab 2015) so far.

Table 2.1.1: Cyber-attack Timeline

Year	Country	Effected Area
1998	United States	Individual Computers
2006	Estonia	Government Networks
2007	United States	Secretary of Defence
2007	China	Government Corporate Leaders
2008	United States	Political Party Database
2008	Georgia	Computer Networks
2009	Israel	Internet Infrastructure
2010	China	Search Engine Baidu
2010	Iran	Iranian Nuclear Program
2011	Canada	Government Networks
2011	United States	State Defence Contractor
2012	Russia, Kazakhistan, Belgium, India, Afghanistan, Armenia, Iran, Turkmenistan, Ukraine, United States, Veitnam, etc.	Key Government Information
2013	South Korea	Government Institution and Private broadcasting company
2014	United States	White House
2015	United States	Office of Personal Management
2015	United Kingdom	Private Companies

Source: Global Research and Analysis Team, Kaspersky Lab, 2013

Figure 2.1.1: Timeline of key Cyber attacks in 2015


LANDRY'S
credit-card breach
ANTHEM INC.
personal information stolen from tens of millions of customers
HALIFAX / BANK OF SCOTLAND
account activities visible for up to six years
STARWOOD
customer credit- and debit-card information compromised in 54 locations
ASHELY MADISON
more than 25GB of user details stolen and leaked publicly
CAREFIRST BLUE CROSS BLUE SHIELD
1.1M members' names, birthdates, email addresses and subscriber information hacked
BITSTAMP
theft of 19,000 Bitcoins, worth more than $5 million
MANDARIN ORIENTAL
customer credit-card data stolen
CVSPHOTO.COM
stolen credit-card and personal information from online photo site
WEB.COM
93,000 customers' credit-card information stolen
SCOTTRADE
4.6M customers' personal, credit-card and Social Security information stolen
HYATT HOTELS
malware infection stole credit-card information
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
TWITCH
user names, passwords and other personal information hacked
ADULTFRIEND-FINDER
personal data stolen from up to 4M members
HACKING TEAM
attackers claimed 400GB in dumped data
HARVARD UNIVERSITY
more than 20,000 records compromised
HILTON HOTELS
malware infection stole credit-card information
EXPERIAN / T-MOBILE
personal information compromised for over 15M customers and applicants of T-Mobile
AMAZON
passwords compromised
ATLASSIAN
up to 2% of the username and password database stolen
PREMERA BLUE CROSS
records of as many as 11.2M customers exposed
OFFICE OF PERSONNEL MANAGEMENT
4M federal employees' personal information stolen
VTECH HOLDINGS
5M customer accounts breached
LIVESTREAM
customer database compromised

Source: Dell Security Annual Threat Report, 2016

The report further warns that attackers are expanding their operation to new areas such as Asia, Middle East, Baltic countries, Central Europe and Africa.

In response to such attacks, efforts are being taken by individuals, organisations, institutions, multinational organisations, and states to pre-empt and secure this highly connected and yet vulnerable space. However, as per the dominant theory of International Relations, all these efforts are considered from the vantage point of state. The most advanced states in this regard are United States, China, Russia, Israel and United Kingdom followed by emerging cyberpower states like Iran and North Korea (Breene 2016).

United States in one of the leading states in this case. Post 9/11 government of United States successfully made Cyber security as its one of the top National Security agendas. In its top down approach United States established National Cybersecurity and Communications Integration Center (NCCIC) under National Protection and Programs Directorate which directly reports to the United States department of Homeland Security. NCCIC key mission is protecting and enhancing the resilience of cyber infrastructure of United States (Homeland Security 2016). The most statist and revolutionary step that United States took was the establishment of United States Cyber Command (USCYBERCOM) in 2009.

It is a subunified command under the United States Strategic Command (USSTRAT-COM) which is aimed at making a full-fledged Combatant and Command (COCOM) in the next five years from its establishment in 2009 (Hollis 2010). The main reason for not going directly to COCOM is that the situation in 2009 would have been so sensitive that a cyberstrike from any adversary needed an immediate response and strike back with the help of Department of Defence (DOD) (Hollis 2010).

This means any cyber attack or threat by any state or non-state actor will be retaliated or deterred in the form of military action which could be joint action between army, navy, air force, and paramilitary forces. In fact, at present each of these forces has their own established cyber command. These developments have set the stage to United States for future *cyberwarfare.* In fact in April 2016, the United States Deputy Secretary for States Robert O. Work publicly announced that USCYBERCOM is dropping cyberbombs against Islamic States (Sanger 2016). Perhaps this is the first time in International Relations history that a state is announcing cyberwar against an adversary. Interestingly, in this case the adversary is not traditional other state, but non-state actor – Islamic States. And, this marks as coming of cyberspace on the centre stage of world politics and International Relations.

Russian experience in securitisation of cyberspace by state began in 1998 when it was gearing up for negotiating an international convention where states should be banned for creating cyberweapons against other states (Demidov 2013). This effort never realised and over a period of time Russia has now moved from defensive to offensive strategy in order to protect and secure its cyberspace (Demidov 2013). Following United States, Russia, in 2013, proposed to bring the various cyber security components under one command (Demidov 2013). That is, establishment of Russian CYBERCOM under the ministry of defence.

Learning both from United States and Russia along with its own experience, the Asian giant, China has been active in formulating strategies and doctrines to develop advanced Cyber warfare systems and tactics. The Chinese have carefully defined the term Information Warfare (IW) when it comes to exploiting cyberspace for its military purpose.

This is well captured Xie Guang, the then Chinese vice Minister of Science and Technology and Industry for National Defence, when he defined IW as:

> "IW in military sense means overall use of various types (of) information technologies, equipment and systems, particularly his command systems, to shake determination of enemy's policy makers and at the same time, the use of all the means possible to ensure that that one's own systems are not damaged or disturbed (Anand, 2006)"

This definition could give China an edge over United States forces against which the Chinese conventional weaponry are relatively inferior (Mulvenon 1999). This is how China is exploiting cyberspace in order to leverage *asymmetric strategies* (Mulvenon 1999) through which it can challenge the much more advanced adversaries like United States. China has been allegedly establishing various cyberwarfare units within and outside its military establishment.

These units are of three types: specialized military network warfare forces, special civilian organisations, and external entities (Harris 2015). First one is unit within the Chinese military which is responsible for carrying out specialised network attack and defence. The second type is group of civilian government organisations which are authorised by the military to carry out network attacks. These are usually the intelligence gathering and investigation organisations which have their established network and support from state as an added advantage in executing cyber attacks. The third one is external organisations and agencies which can be mobilised and instructed to carry out cyber operations as and when required. These three units ensure that the information technology talent and resources for the state is utilised appropriately against any external threat. This model of military collaborating with the civilians and external agencies is a strategy well planned for the state's defensive and offensive security of cyberspace. However, Chinese military is now considering bringing all the scattered cyber capabilities under one command similar to the United States (Shi and Zhai 2015).

There is clear trend in all the above mentioned cases where state's take on securing the cyberspace is bending more towards military use.

Although there is collaboration with the non-state actors like organisations and agencies, clearly this collaboration and co-creation is working towards making military continuously more powerful in launching cyber attacks and promoting cyberwars. It is not to acknowledge that this will bring some phenomenal innovations and developments in cyberspace technology and policies, but these developments, in long term, eventually will ensure that states engage in the unidirectional path wherein the other important development aspects of cyberspace at social and humanitarian level would be neglected or unattended.

This means that Cybersecurity will eventually be reduced to the typical traditional security narrative. And, this virtual space of electronics, machines, and devices, is soon turning to be a contested space among the states accompanied by advanced military weapons.

Also, the shift from defensive to offensive stance in Cybersecurity policy is worth noticing. This stand by advanced states is disturbing to the overall long term good of cyberspace. This builds more mistrust among the states making the entire world system volatile and highly sensitive. It is therefore no doubt that the Cybersecurity policy documents and doctrines of these nation-states are flooded with the words like *Cyberdeterrence*, *Cyberwar*, *Cyberdefense*, *Cyberpower*, etc. Eventually, exploiting the cyberspace, which would otherwise have the potential to bringing the world together and closer to each other, to the extent that it becomes more divided than ever.

Copenhagen Securitisation of Cyberspace

Copenhagen school, as discussed before, greatly emphasises on the ‘speech act’ by securitising actor and its influence on the audience about the existential threat by referent subject on the referent object. Much of this has been discussed in detail in the first part of this section. In this section the objective is to understand to analyse and understand the securitisation of cyberspace as per the Copenhagen school and draw out the implications and the relevance to the broader theme of the chapter. As stated before, Copenhagen securitisation is seen as negative securitisation as per the working definition of the securitisation in this paper.

In his mixed method analysis of securitisation of cyberspace in case of United States, Ola Hjalmarsson (2013) analysed few dominant speech by leaders like president Obama and quantitatively analysed about ten thousand official documents from the departments like Department of State (DOS) and Department of Defence (DOD). In his study of speech texts by U.S. President Barrack Obama and the then Secretary of Defence Leon Panetta, he found 'hypersecuritisation' of cyberspace. This was being carried out by representing that there is constant threat to the connected referent objects under cyberspace from the adversaries. Images of past catastrophes such as September 11 and Pearl Harbour were being used to invoke a sense of immediate existential threat to the connected referent objects in cyberspace. This way U.S. government gets the affirmative node for immediate action plan in order to protect the sovereignty of the state. Complementing this, his quantitative analysis also pointed to the fact that the government documents frequently used the words like cyberspace, cyber, defence, military, network, security, computer, systems, etc. In fact, he found that the word "security" was the most frequently associated with the word 'cyberspace'.

The action plan that United States executed in response to these unverified claims of threat in terms of heavy investments and high resource allocation was seen as securitisation and militarisation of cyberspace (Hansen and Nissenbaum 2009).

In fact securitisation of cyberspace in Europe is not different. Immediate elevation of Cybersecurity from low politics or normal agenda to national security is questionable (Guitton, 2013). This is because: Firstly, the justification put forward by these states for such immediate response did not hold correct. The action plans were taken completely based on the experiences and the responses of other state like United States, non-classified information and false statistics. There was no verifiable evidence other than quoting fictional movie scenarios and past incidents which were remotely related to real cyberspace attack. Secondly, the security frameworks by these states to address the cyber attacks were more coherent to their national security strategies. That is rather than addressing the growing cybercrimes and attacks these frameworks were directed towards state's adversaries. Rather than looking inwards to the cybercrimes originating from within their own state these strategies are more outwards oriented. And finally, these responses from these states were taken primarily to address the insecurities from the growing cybercrimes and threats for which the source or origin has always been difficult to identify.

During framing these strategies there was no concrete evidence that the adversary states of these three countries directed the various cyber crimes and attacks. And, it is because of this rather than deterring the cybercriminals and attacks, these frameworks work to mitigate the impact of cyber attacks by unidentified criminals.

Such response from states on securitisation of cyberspace as national security is detrimental to the referent objects other than state. Cyberspace constitutes a series of well interlinked referent objects of the individual, the state, the society, the nation, and the economy (Hansen and Nissenbaum 2009).

Most importantly, this non-focus on the people oriented securitisation of state to militarise cyberspace and grab cyber power has compromised the security of the individuals (Cavelty 2014) and the voice-less. And, paradoxically, this growing securitisation of cyberspace as a part of national security is making the world cyberspace more vulnerable and insecure (Cavelty 201).

Consequences of Cyber securitisation on unheard-voices

As mentioned above, the dire consequences of securitisation of cyberspace is not just limited to increasing gaps between the states, but it also has deep impact on all other interconnected referent objects under the sphere of cyberspace. Most importantly on the individuals (as an integral part of larger system of state and international society), unprivileged communities, socially excluded groups, and other marginalised section of the larger international society.

Freedom of expression transcending nation-state boundaries with the help of Internet was what cyberspace was initially seemed to be promised. With the wide potential of connecting people through networks bypassing the physical limitations, it was a new sensation of hope for all the people, especially the unheard voices and marginalised, where one could easily express thoughts and views. However, with the intervention and direct control of this space by state, this freedom of expression is greatly compromised.

In 2012, Shaheen Dadha, a girl from Mumbai, posted a Facebook status criticising the shutdown of Mumbai city on the funeral of Shiv Sena chiel Bal Thackray (Press Trust of India 2012). Her friend Renu Srinivasan liked status. Both Shaheen and Renu were arrested by Mumbai Police under the Section 66A of Indian Information Technology (IT) Act. Since the year 2012, there were more than ten cases where individuals were arrested or booked under Section 66A of IT Act for allegedly posting comments against the state or representative of state in social media like Facebook (Hindustan Times Correspondent 2015). Although after three years, Supreme Court declared this section as unconstitutional and struck it out from the act, there are many such cases of individual's freedom of expression and right have been censored and controlled by the authorities of Indian state. In the last half of the year 2015, Facebook received 5561 requests, highest since its operation in India in 2013, on user data from Indian authorities (Purnell 2016). Worldwide level, United States leads with the highest number of requests (19,235) for user data in Facbeook (Purnell 2016).

For instance the "Great Wall of China Firewall" constantly monitors internet activity of Chinese netizens and blocks websites and web-based mobile applications which Chinese government considers as threat for state (Amnesty International: n.d.). Recently, a Chinese activist, Shi Tao, was convicted for anti national activity and sentenced to 10 years of jail (Amnesty International: n.d.). All he did was that he sent email to a pro-democracy group about 15th anniversary of Tiananmen Square. Also, close to 3000 websites like Amnesty's international site, google.com, Picasa, Facebook, YouTube, Twitter, Blogspot, Instagram, The independent, etc. are blocked in China (Wikipedia n.d.). In fact, under the leadership of president Xi Jingping, China recently announced new law to control websites in China (Mozur 2016). Although, the details are not very clear, the violators would be fined $1,500 to $4,500. This is in line with its recent policy of centralisation of cyberspace in China when it launched cyberspace Administration (Mozur 2016).

The censorship on region of Tibet, an ethnic minority in the western China, is one of the living examples of how securitisation actually snatches freedom of expression and making view point within the region of Tibet. In 2008 when the riots broke out in Tibet over the consecutive self immolation of Tibetans, the Chinese government imposed total internet control to the region. That is when YouTube and Google were blocked in China so that video clips and pictures from Tibet could be stopped from spreading across rest of the China and world.

All the private media houses were instructed to produce news and blogging materials in line with the state owned media like China Central Television and Xinhua news. Again, in 2012 when clashes broke between the peaceful monks and the Chinese army in Sichuan, the internet service and media channels from the region were blocked (Branigan 2012).

In fact Google pulled out from China in the year 2010 after it was forced to censor as per the Chinese law (Waddell 2015). Since then search on Tibet, Dalai Lama, Tiananmen Square, etc. is strictly filter on the Chinese equivalent of Google, Baidu.com, which is now most used search engine in China.

Another case of securitisation of cyberspace in China is the region of Xinjian. Originally and Islamic region, Xinjian has been under turmoil since thousands of Han Chinese population started migrating from mainland China to Xinjian. In October 2013, during Urumqi riots hundreds of Uygurs were detained by police for spreading online rumours (Roney 2013). Last year cyber surveillance reached its peak when the mobile service in the region was shut down fearing the use of mobile applications that by pass the government's virtual cyberwalls (Mizor 2015). The text that one of the mobile subscribers received was:

> Due to police notice, we will shut down your cellphone number within the next two hours in accordance with the law. If you have any questions, please consult the cyberpolice affiliated with the police station in your vicinity as soon as possible (Mizor 2015).

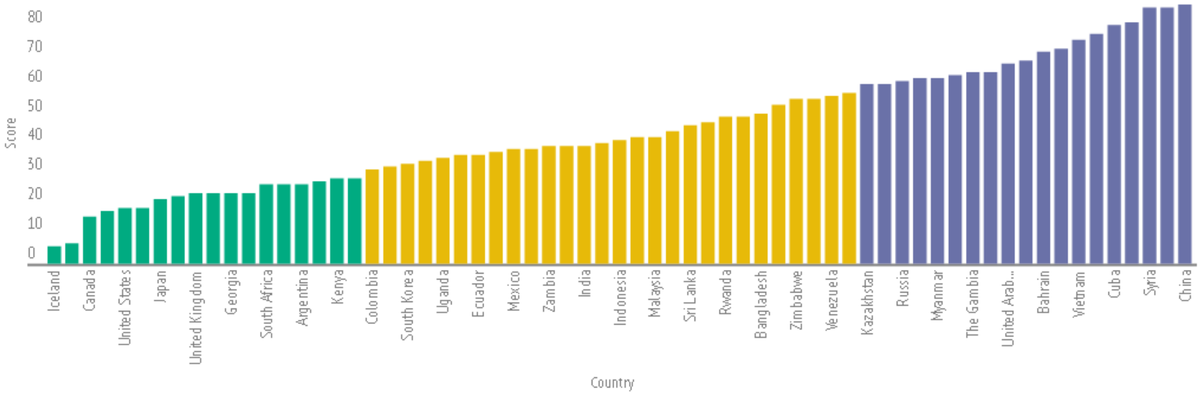
Therefore, China, as a state, is leaving no stone unturned in order to suppress the voices coming from the minority regions likes Tibet, Xinjiang and Inner Mongolia by means of direct infringement with the freedom of expression in cyberspace.

And it is not surprising that the state is ranked one as the worst Internet free country in an exhaustive report titled 'Privatizing Censorship, Eroding Privacy: Freedom on Net 2015' by Freedom House, an independent freedom and democracy watchdog based in United States.

A detailed ranking of the participant states in the survey by Freedom House (2015) is shown in the Figure 2.3.1. Green colour represents 'free' internet, yellow represents 'partially free', and purple represents 'not free' Internet. The most censored topics (which are explicitly state sanctioned) are criticism of authorities, corruption, political opposition, satire, social commentary, blasphemy, mobilisation for public causes, LGBTI (Lesbian, Gay, Bisexual, Transgender and Intersex) issues, ethnic & religious minorities, and conflict (Freedom House 2015). The censorship includes blocking of a relevant topic from websites, initiating trackdown and deletion requests, or arresting users for writing on that topic in the various online forums like blogs and discussion forums.

Although, these crackdowns are directed towards a particular community based on religion, identity, gender, economy, or political ideology, ultimately the final touchpoint is the individual representing the community. The report Freedom House (2015) accounts the following incidents. In Morocco, 17 year old rapper Othman Atiq was arrested and detained for few months after he criticised the police in online video. A 25 years old man was sentenced to seven years in jail for sharing a satirical song through his mobile in Bangladesh. An Iranian cartoonist was sentenced to 12 years of prison for making cartoons where political leaders were depicted as animals. A transgender woman in Egypt was sentenced to six years prison after she share video her dancing in YouTube channel. Lebanon blocked a lesbian forum which was used all over the Arab region for discussion on the issues related to lesbians. Vietnam blocked contents promoting the religious groups like Buddhism, Christianity, and Cao Dai and in UAE a forum for Christianity was blocked. Apart from this list there are innumerable accounts where the individuals were arrested and detained for expressing their views online.

Figure 2.3.1: State Internet Freedom Score Comparison



Source: Privatizing Censorship, Eroding Privacy: Freedom on Net 2015

Figure 2.3.2: Protestors demonstrating against internet censorship of China during CeBit computer trade fair in Hanover, Germany (March 2015)

Unable to connect to Human Rights
Meinungsfreiheit ist in China
nicht verfügbar

Source: Privatizing Censorship, Eroding Privacy: Freedom on Net 2015

Chapter 3

INCLUSION IN CYBERSPACE AS EXCLUSION OF MARGINALISED: A PARADOX OF GLOBALISATION

In 2011, the United States technology giant Apple sold 70 million iPhones worldwide and none of them were made in United States (Kabin 2013). Here is how Apple iPohones are manufactured. Design, software, core parts and marketing are all done in United States, rare earth materials are sourced from China and Inner Mongolia, memory chips and display screen are made in South Korea and Taiwan, a French-Italian company manufactures gyroscope for screen's auto-rotate feature, and 85% of the phones are being assembled in China. This is a snapshot of how one product is being manufactured under the process of Globalisation.

Globalisation is a worldwide phenomenon that has been making the world smaller with the help of massive development in information, technology & communication (ICT) in the last few decades. In doing so it is also increasing interactions and contact between people from different parts of the world, which would not have possible in pre globalisation period. These interactions are taking place at all levels of world system. That is at individual level, community level, society level, organisation level, state level, and world level. And this platform for interactions, meeting points and sharing of materials is provided by cyberspace. One cannot imagine globalisation without cyberspace. However, behind this rapid development under globalisation one needs to be careful about the irreversible damage it is producing on some sections of the international society, community and individual. These sections of the population are poor, not well materially developed, unprivileged, uneducated or excluded ethnic groups, tribal aborigines, rural dwellers, LGBTIs' and so on. The damage, as far as the impact of cyberspace under the umbrella of globalisation is concerned, further excludes these marginalised population away from the agenda of involvement, participation and engagement with the mainstream international system.

Globalisation

Globalisation, as the name suggest is the process related to a global phenomenon. It is defined by United Nations Educational, Scientific and Cultural Organization (UNESCO) as:

> ...ongoing process that is linking people, neighbourhoods, cities, regions and countries much more closely together than they have ever been before. This has resulted in our lives being intertwined with people in all parts of the world via the food we eat, the clothing we wear, the music we listen to, the information we get and the ideas we hold (Fien n.d.).

The definition above includes all discipline that one can imagine. Be it economy, science & technology, politics, social science, environment & ecology, medicine, art & culture or developmental studies. As result, in academic literature there is no one broad definition and understanding of the term; every discipline defines and understands globalisation within its own lens (Mooney and Evans 2007). Consequently, it is a contested term where every discipline argues in favour of its own understanding of the term within the limits of its discipline. However, Oxford English dictionary defines the term as the 'process by which business start operating on a global scale' (Oxford English Dictionary 2012*)*. Here the phenomenon is associated with business and economy. It is no secret that the presence and influence of corporate multinational companies and organisations is being felt almost every part of the world. Perhaps there is no city left today where there is no presence of McDonalds, KFC, Coca-Cola, Google, Microsoft, Samsung, Apple, Nescafe, Sony, Lenovo, Nike, Reebok, etc. Even among the general masses it was found that the term is usually associated with the big business and economy (Mooney and Evans 2007). Although there is no clear reason for this, it is pretty much understood these visible brands are strong enough to make the people give a perspective of being a global. One of the most downloaded android English dictionaries called Word web dictionary, which has so far one million downloads states globalisation as 'growth to a global or worldwide scale'. This is very open ended definition where any of the discipline can build up more to refine more focused definition of the term.

While there is dispute over the definition of the term, there is equal debate over understanding the *pros and cons* of the phenomenon (Dreher et al. 2008). And this is quite natural as every discipline will understand the consequence of globalisation from its own perspective leading to different conclusions (Dreher et al. 2008). Therefore, a well encompassing definition of the term becomes important to avoid any confusion or conflict between the research scholars. One such encompassing approach of globalisation as defined by Dreher et al. (2008) is follows:

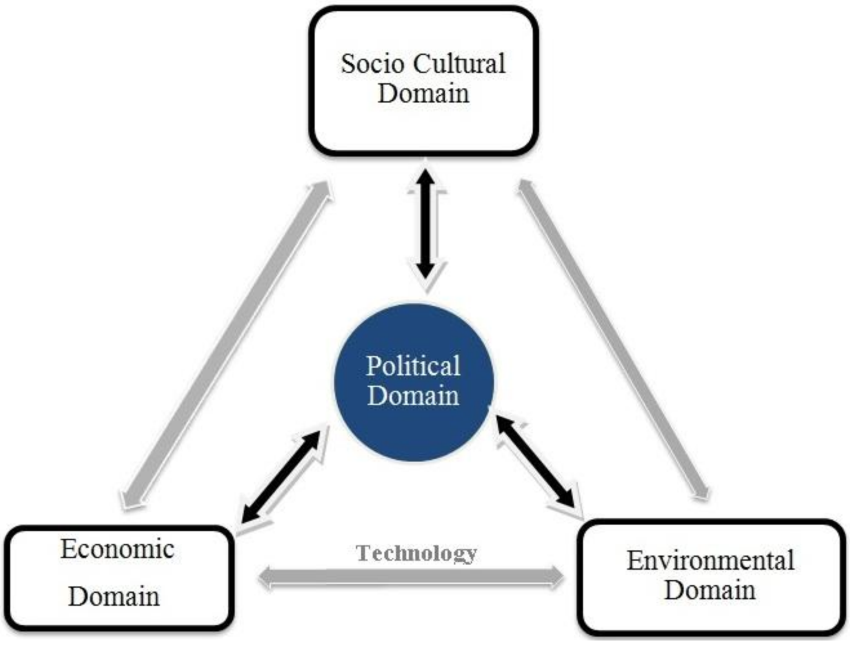
> Globalisation is the interactive co-evolution of multitudinous technological, cultural, economic, political, social and environmental trends on all conceivable spatiotemporal scales

Figure 3.1 shows the plurastic model of globalisation as an over-arching process in which different processes takes place simultaneously in various domains like Socio-culture, economy, environment and politics (Dreher et al. 2008). It is to be noted that technology plays mediating role between the socio-culture, economy, and environment domains.

Political Domain

The political dimension of globalisation is as important as the economic domain. The various form of political structures and ideologies have very much shaped globalisation process. Liberal forms political structures very much contributed in building right environment for economic development. More liberal states began to participate in international trading under various conventions and mutual agreements. states like United States motivated many other democratic states to become developed state. Had it been any strictly conservative state like North Korea, the process of globalisation would not have been possible.

Figure 3.1.1: A pluralistic approach to globalisation



Source: Dreher et al. (2008)

Economic Domain

As mentioned before, the domain of economy is mostly associated with globalisation by general people. The process is important from the fact that this generates wealth which is one of the basic essentials for living for everyone. Two important events can be considered important towards the process of globalisation (Dreher et al. 2008). The first one is discovery of America which represents colonialism. And, the second one is the establishment of first multinational company called Dutch United East India Company in 1602. This emergence of multinational heralds the start of capitalism as the most prevailing economic system in the world. The company had started the custom of multinational trading system with the help of his trade ships. Eventually, various developments took place with the rise of multilateral, bilateral and regional economic initiatives among the states and the multinationals. The various forums such as World Trade Organisation (WTO), European Union (EU), etc. started contributing more to the global economic innovation and change. Therefore, it can be said that economic domain provided the initial thrust for globalisation.

Technology

As technology is the mediating factor among all other domains, it becomes as important as any other domain. Technology has immense power of brining strong waves of change in the direction of globalisation. One of the major breakthroughs in technology that lead to globalisation is the invention of steam engine and electric telegraph in 1800s' (Dreher et al. 2008). Both revolutionised the way people travel long distance journey and connected people together for trade and business. Another important turning point was the invention of rocket propulsion by German engineers (Dreher et al. 2008). With the help of this, states could send satellites in space and improve electronic communication channels resulting in to reliable and global communication. Perhaps it was a historic moment where for the first time truly globalised and reliable communication system could establish (Dreher et al. 2008). And the most revolutionary technological innovation which contributed most in globalisation is the invention of computer. In 1971there was a leap in the processing capability of computers when Intel invented microchip. And, with this the development of ICT also got shot up as mode of communication became much easier and faster.

Socio Cultural Domain

Interaction between the processes of different domains like technology, politics and economics has resulted into movement in social and cultural domain. The rise of multicultural societies can be seen as an outcome of such process. With the growing connectivity among the people through various media like television, social media, internet reports, live updates, newspapers, and radio there is rapid cultural exchange among the societies all over the world. The western culture, especially American, has been widely adapting by many developing states including India. One of the most influential channels is Hollywood, which has been successfully marked its presence all over the world. This results in spreading the American way of life and culture to other societies in the world. The widely celebrated television comedy serial like *Friends* has completely inspired many youths from developing states to adopt living style that serial used to show. The recent rise pop culture from Korea, popularly known as K-pop, is taking Korean culture across other Asian and European states. The youths in some parts of Asian states like India, Nepal and Bhutan are now seen adopting Korean culture and dress in order to assert their fashion and young age in society. Having said so, the picture of socio cultural change in regard to globalisation is not always positive. Recent rise of orthodox groups and extremist political parties depicts the negative side of the socio cultural change of globalisation. The rise of Islamic States (IS) with the assertion of creating a state based on Islam and the havoc that it has caused in the Middle East region one such example of other side of globalisation. Also, in response to this, extreme migration laws against the influx of people leaving their homes from the fear of IS to neighbouring European states is worth worrying.

Environmental Domain

Recently in a fundraising event Hollywood actor Leonardo DiCaprio said that present generation is the first generation that has the technology, the scientific knowledge and the global will to build a truly sustainable economic future for all humanity and also the last generation that has a chance to stop climate change before it was too late (Chow 2015). His remark captures the urgency of the situation that our environment is facing due to our incessant quest for development.

Although the process of globalisation does not necessarily harm our environment, certain process of various domains discussed before has certainly exploited the very earth that we all live on. For instance air pollution due to increase in modes of transport systems, deforestation, and release of toxic gases from factories; water pollution by dumping industrial waste in rivers, directing city sewage into the nearby water bodies, house sewage being directed to and stored below ground level affecting underground water. Cumulatively, all these pollution are causing adverse impact to earth's climate causing several natural catastrophes like flood, earthquake, volcano, and forest fire. It is directed by most that there is direct correlation between climate change and globalisation (Dreher, et al. 2008). The rise of sea levels in low areas leading to the shrinking of already habitable land, rising number of ecological refugees, reducing surface area of glaciers, acid rains, and frequent flash floods are forcing everyone to address the ill effects on globalisation on environment.

Globalisation and Cyberspace

Since technology act as mediating factor between all other domains of globalisation process one can say that cyberspace, as a product of technology, is one of the most widespread platform or space (virtual) where the processes of all other domains takes place. This virtual space has become the platform where the economic, political, socio-cultural, and environmental domain of globalisation interacts and converges. For instance trading today has been completely digitalised in the various well known stock exchanges.

For instance, a trader today does not necessarily go to the stock exchange office and trade, rather the person can sit anywhere in the world where there is internet connectivity and by just signing in the particular stock website or application buy and sell of stocks can done. If required the trader can immediately talk to any financial adviser or securities adviser by using internet voice chat applications like Skype, WatsApp, or Facebook Messenger. The trader also keeps an active watch on national or international news (live or non-live) by following news websites, live video applications, or online radio.

This entire process of trading involves the execution of processes of various domains under the space created by ITC – cyberspace. This shows how a trader participate in trading without going to the physical office location, speak to other people using telecommunication devices or internet, and know about the happenings around the world

Interestingly, with the globalisation of internet, cyberspace is also globalising. That is cyberspace is becoming a worldwide phenomenon and it is reaching out to many individuals all around the world, digitalising anything that comes on the way.

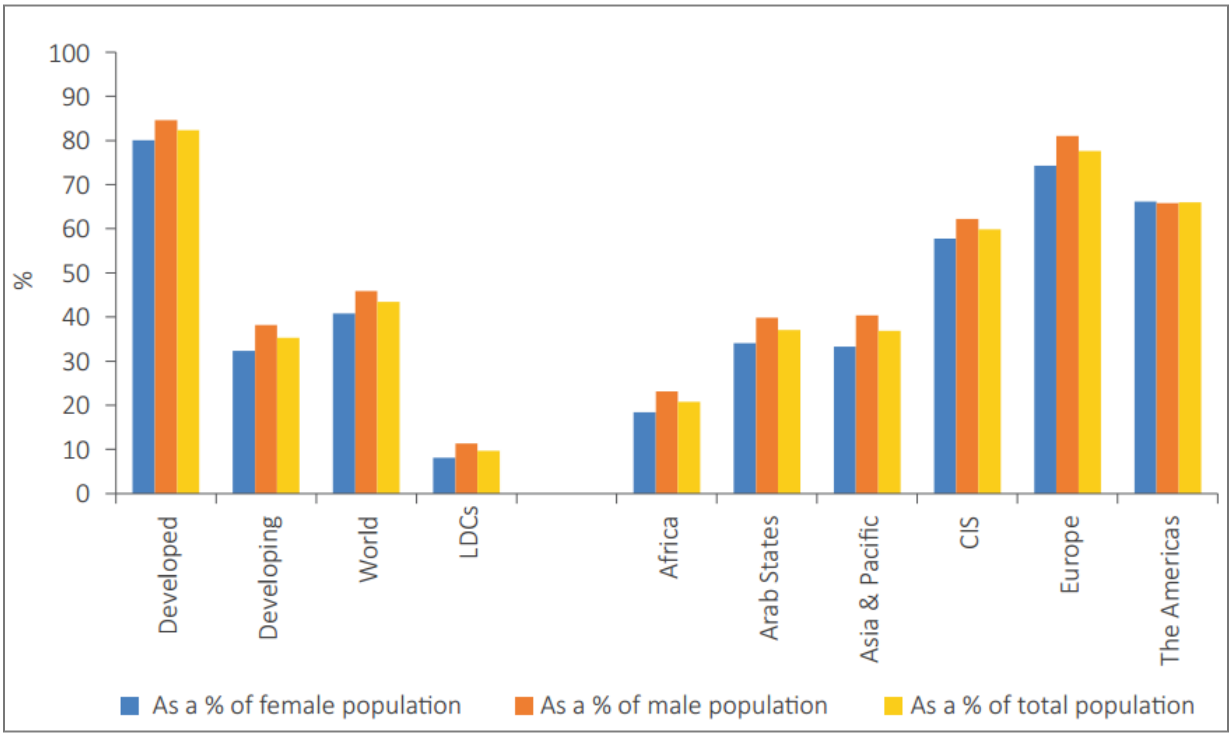
However, as per the statistics it is clear that this spread of cyberspace around the world has been uneven with differences across continents, states, class, gender, ethnicity within regions and nations (Globalizing Cyberspaces n.d.). Also, it is clear that the impact of ever expanding cyberspace have varied tremendously, especially between the people from western states whom have benefitted from the digitalisation, and the people from poor or developing state who have suffered immensely under the guise of digitalisation. Those who have suffered under the globalisation of cyberspace have used the same tools and techniques of cyberspace and technology in order spread awareness among the world by raising their voice and concerns across transnational society.

Digital Divide: An exclusion of Marginalised

The concept of Digital Divide gained momentum during 1990s during the time when the Internet and dot-com booms were making headlines across the world (Warschauer 2003: 11). Various surveys and studies in United States and European nations clearly depicted the growing level of inequality in the use of ICTs – especially the use of computer and internet. This gap was found to be between those who have access to information and those who do not have or ‘information rich’ and ‘information poor’ (Selwyn and Facer 2010).

The figure 3.2.1 shows the worldwide digital divide based on development status of region. As much as about 80% of the population in Europe has access to internet, whereas, in Africa merely 20% of the population has access to internet. And this is almost similar in case of the development status as well. There is difference of around 40% between developed and developing states.

Figure 3.2.1: Percentage of individuals using the Internet by gender, development status and region, 2015



Source: Measuring the Information Society Report 2015, International Telecommunication Union (2015)

The Least Developed Countries (LCD) has the most severe deficit of internet users. This clearly shows that there is direct link between the development status and the internet users. It can be inferred here that the accessibility of internet is still a privilege of the ‘Haves’. While the unprivileged or developing states, especially the LCDs remain far away from accessing cyberspace.

Analysing the users based on gender, percentage of female population of internet users are relatively less than that of male population. However, this difference is negligible in all the categories.

However, many scholars have posited that this divide is no longer restricted only to access of information alone (Segev 2010). Digital Divide today is evolved from the complex process of globalisation where economic, political, socio-cultural, environment and technological factors do play major role. All these factors intertwined and converge towards creating ICT policies and laws that eventually gives a very complex picture of Digital Divide. This not only has created inequality between individuals, but also all other levels of analyses such as community, society, region and state (Segev 2010).

As had been a notion that individuals from the states that are developed, economically superior, and have superior ICT are free from such divide. Perhaps this is time to break away this notion as even in advanced ICT state like United States there is inequality among the individuals. For instance LGBTI related contents on internet are continuously monitored and suppressed by the various extreme political and religious groups even in ICT advanced states. The main reasons for such kind of developments in advanced states are twofold. Digital divide caused by commercialisation and politicisation of cyberspace where dominant websites and channels do play key role. Second, information generated in the network of internet is largely dependent on information-skilled users (Segev 2010). In spite of being one of the most democratic and multicultural states in the world, it was found that digital divide between different ethnic groups still prevails in US.

Blacks and Hispanics are mostly found to be offline compared to other ethnic groups where as the whites are the ones present in highest number in cyberspace (Losh 2010). Similarly, there is digital gap among the poorly educated section of the American society. On the other hand the Internet access with high speed home connection is disproportionately concentrated among the rich whites and educated Asian-Americans. Similarly in another study by Linda (2010) on digital divide in US, it was found that the 'haves' side of the divide has seamlessly fit their daily activities with the high speed 24/7 internet connectivity. They use internet in order collect information on various topics of their choice from simple 'how to' searches to politics and economy. The youths engage themselves into highly engaging and sophisticated online games and which are entertaining as well as educative. They even extract academic information from the internet resulting into better performance in their schools and colleges. On the other hand, the "have-nots", are deprived of such facility which is not only essential for their academic performance but also their awareness and participation in politics and society. Thus, the rich would keep accessing the already excess information from internet and the poor would be further pushed to the corner with no way to access information.

Having said so, the focus here is the prevailing exclusion of marginalised population from the larger international social and political society. The marginalised related not only to the traditional definition but includes all sections of individuals who are on the fringes of mainstream socio-political area. These includes poor, unprivileged low caste sections, uneducated and illiterate, old age people, LGBTIs, disabled, and ethnic groups, aborigines and tribal groups.

Chapter 4

EMANCIPATION IN CYBERSPACE

What is Emancipation?

Emancipation in dictionary is defined as ‘free from legal, social, and political restrictions or free from slavery’ (Oxford English Dictionary 2012). That is, emancipation is about freedom from the restraints of legal, social and political bindings. It is about being absolutely free from the limitations of restraints around us. Another perspective of emancipation is the one propounded by the founder of Indian constitution Dr. B. R. Ambedkar. His idea of emancipation is the liberation of people in India who were oppressed under the tradition of caste system in Hindu religion as untouchables. For Ambedkar the greatest emancipatory path is knowledge and that is why he stressed on education all the time. He did not shun away the existence of the community, society or state. Rather for him emancipation within the ambit of social constructions of society, community, religion, state and international system was more important than an absolute emancipation.

In International Relations, however the term is coined first by Ken Booth, his definition of the term emancipation as a ‘discourse of politics’:

Emancipation seeks the securing of people from those oppressions that stop them carrying out what they would freely choose to do, compatible with the freedom of others. It provides a three-fold framework for politics: a philosophical anchorage for knowledge, a theory of progress for society, and a practice of resistance against oppression. Emancipation is the philosophy, theory, and politics of inventing humanity (Ken Booth 2007).

As mentioned above, emancipation is conception of being free from all the physical and mental constraints by an individual. Its understanding depends on the notion of freedom. Ken Booth (2007) states that it is the true freedom and not the false freedom that is associated with emancipation. False freedom comes with the negative human side in the form of freedom of doing anything that cause non-violence and harm to other human beings. The true freedom is the one where the positive side of human mind is reflective. This includes the notion of freedom to execute anything which does not harm others. In emancipatory security, individual and human freedom takes precedence over state and power (Booth 1991). This is beautifully explained by Ken Booth (1991) by stating that individuals should be considered ‘as end and not means’. state and all other non-human related entities should consider as means to attain emancipation of individuals. It is therefore can be understood that the very objective of emancipation primarily secure people from all kinds of oppression that restricts them from doing what they freely like to do without any fear. That is why there is non-dual relationship between security and emancipation (Booth 1991). That is, security must be treated as a means to achieve emancipation, and emancipation should be used to achieve security.

Also to be noted is the three pillar framework for politics; ‘philosophical anchorage for knowledge’, ‘theory of progress for society’, and ‘practice of resistance against oppression’ (Ken Booth 2007). Philosophical anchorage for knowledge is defined as the best and most authentic knowledge of what is true and not. This knowledge, therefore, cannot be taken lightly as this knowledge is about truth and it is based on this knowledge of truth that the future course of action would be undertaken. The second pillar is about understanding actual condition of the word politics. The last pillar is about practice of resistance against oppression. It is considered as the framework for actualising both near-term and long-term emancipatory goals. This practice of resistance is executed by the tactical and strategic political action, largely driven by inherent critique.

Taking a balanced position from the two above discussed understanding of emancipation, the concept of emancipation can be defined as an endeavour by which an individual or all its larger functional systems (like community, society, group, state, nation, etc,) can be rescued or secured from a position of extremely inhuman, unfair, unjust sate of being to a position where human dignity is restored and respected. And in doing so, no other individual or its extended larger functional system should be deprived of its basic freedom towards such endeavour.

In the above definition, emancipation is not just restricted to individual. It is in fact, extrapolated to other functional systems of individual. This inclusive definition of emancipation is considered because individuals cannot completely dissociate from the construction of systems like community, society or state.

An Emancipatory Securitisation in Cyberspace

E*mancipatory securitisation*, as derived in chapter one, considers individual as its primary focus whereby mobilisation, by a securitising actor, of the audience takes place with the view that emancipation of individual is the primary important objective. This consideration of the individual does not necessarily do away with the invalidity of the state or any other higher collective form as a system. Because when it comes to cyberspace it is difficult to separate the constituents of a system from the larger body of system. The definition is well grounded on the three pillars of emancipatory strands (philosophical anchorage of knowledge, theory of progress for society and, and practice of resistance against oppression). These pillars protect individuals from any kind of threat from the authoritative governments. It ensures that progress of individuals as a part of larger international system. This can be taken as given as the underlying objective of emancipatory action is not to constraint or chain any individual.

And, in doing so the emancipatory securitisation eventually leads to the emancipation of all.

Digital Social Movements

Whenever the state or any authority of power or influence tried overpowering the individual there has always been cases of response from the online community against it. However, the intensity and the tactics of such response decide the fate of the initiative. In some cases they are stopped and silenced immediately and in some cases they become national or global social movement. And, despite state being powerful both economically and military there are emancipatory movements in cyberspace that penetrated the walls of the rigid state and crushed the orthodox and inhuman power of state which disregarded individual live and freedom.

There are number of reasons why such digital movements are becoming successful. First important factor is *Connectivity*. Behind success of large scale digital movement is the use of social media like Facebook, twitter, etc. which made it possible to connect instantly with the masses and spread the message or point of view across.

Such movements which use social media for mobilising the audience are called Networked Social Movements (Western 2014).

Second factor is *Mobilisation Power*. This unique feature of mobilisation power (Eric Tunner 2013) of cyberspace equips digital movements with a powerful drive to reach the masses at great ease within very short span of time. This makes securitisation process indeed very effective as reach and time are the deciding factors that affect securitisation process. Another feature of such movement is the ability to influence 'offline' masses too (Eric Tunner 2013). It is no doubt that the networked social movements reach out to its 'online' audience, but at the same time it has tremendous potential and ability to reach and influence those who are not connected to cyberspace. This is because most of the time any topic in the form of a video, image, sound, or texts that goes 'viral' in internet on the platforms like YouTube, WatsApp, Facebook, Snapchat, etc., is being discussed by print media and by words of mouth too.

For instance, in early 2013 a short video in which a group of young people are seen dancing on the song 'Harlem Shake' went viral. The video was replicated many other people and it filled the space of social media gaining a widespread popularity among the internet users. In just 40 days after the video was released , it was viewed by 1 billion people across the world. At its peak 4000 version of 'harlem shake' video would be posted on internet. Soon print media started capturing news of 'Harlem Shake' dances being performed by various popular groups across the globe. In March 2013, just after one month of the video release, Australian miners were fired from their jobs for dancing on 'Harlem Shake' and posting on YouTube (The Guardian).

The third important factor is *Anarchical Nature* of such movements. In Networked Social movements there is never an identified leader as every individual who is associated with the movement feels equal and on par with any other individual. The whole moment moves with a collective effort where nobody is a leader and nobody is a follower. A leaderless movement based on a single cause and collective value becomes attractive for anyone to participate, especially the youths.

This is emancipatory as such model does not identify anyone as leader or follower, rather the movement considers everyone as equal and ask everyone’s participation to free the individuals against any oppressive agent or system, be it state or anything else. In fact, Western (2014) defines the term ‘Autonomists Leadership’ which is a collective leadership format.

#YoSoy132

#YoSoy132 was a student moment on cyberspace which drew international attention after it successfully exposed the state’s involvement of producing fabricated message and news with the help two giant media house (Treré 2015). The movement sparked when the leader of Mexico’s ruling party National Action Party (PAN), Enrique Peña Nieto outrightly justified the police repression in Atenco that took place in 2006. At that time Enrique was the Governor of Atenco. The students in the Universidad Iberoamericana in Mexico City to whom he was addressing the justification booed him down and continued their peaceful protest. They were subsequently labelled as thugs, violent, and agents of left parties by the political leaders of PAN. This was widely covered by the two media giants who further accused the university students as the conspiring against the PAN candidate for upcoming election (Treré 2015).

Against this manipulated coverage of the media as many as 131 university students made a YouTube video revealing their identity and personal details and uploaded on the internet. The video went viral and subsequently students in show of their solidarity with the movement started the hashtag #YoSoy132, which means ‘I am 132’. #YoSoy132 went on to become the name of the entire movement (Treré 2015). The moment’s key objective was to bring democracy back into the state’s media. It was later found by international press that the leader Enrique’s image was strategically planned and developed over six years by media group along with the political party that he lead.

To some extend the moment started by students ensured that their voice was heard not only by the people of Mexico but by the entire world. The students during the entire movement were constantly in touch with each other by using social media and chat services like WhatsApp. This back stage discussion on the movement was associated with Mexican rebellious tradition, thereby gaining legitimacy among the others who wanted to join the move.

These discussions and chats reminded the students about the Mexican past and inspired them to become revolutionary by participating in the movement. Had it not been the social media and web technology 2.0 such seamless communication and mobilisation of people would not have been possible; especially in a state like Mexico where violence is prevalent all the time and where the state machineries were broken and complete failure.

The #YoSoy132 movement, therefore, suddenly empowered powerless university students and gave confidence in the power of cyberspace to all those individuals who feel helpless and minute in front of state. This confidence can easily be associated with the notion of emancipation where every individual, irrespective of role or position, feels fearless and confident about anything that concerns progress and goodness of the individuals.

Tahrir Square

In 2011 thousands of people from all walks of life gathered at Tahir Square, Egypt, demanding end of authoritarian President Hosni Mubarak's rule. Inspired from Arab Spring, people were protesting against the lack of free election, corruption, rising unemployment, brutality of police and military on the civilians, high food inflation, and low wages. The movement got a boost when, for the time in the history of world, internet in the entire state was blacked out (Cattle 2016). This move by the state was in response to the use of cyberspace, especially social networks like Facebook, Twitter, etc., to mobilise people for the protest. During the clash between the protestors and the police hundreds of protestors were killed and thousands of them were injured because of brutal attack by the state police. State emergency was declared in Egypt as the state was undergoing one of the biggest ever political mass uprisings. Eventually, after eighteen days of continuous protest the citizens of Egypt successfully remove Hosni Mubarak when he stepped down on 11 February 2011.

Once again this success of people clearly showed that cyberspace facilitated online expression, discussions on issue, exposure to external resources, netizen journalism, association of people from varied parts of life with common view, empowerment of women and minorities, and reporting on human rights abuses (Cattle 2016).

Net Neutrality – a case of India

Net Neutrality means that internet users can access internet in freely without any restrictions or restrains on the type and nature of the content as long as they are within law of the land. This means a service provider should not block access to any content, websites, and applications and allow the users to access everything on internet irrespective of the source as long as it is legal (Khadekar 2015). It also includes no differential rates to the service of Internet by the internet service provider or telecom company. Also important is the level playing field on the internet. That is, there should be no biased treatment to any of the websites or applications in terms of speed or access. Every website or services online should co-exist within the context of cyberspace without causing any harm to others. And, no particular websites or applications should run at any biased speed. When on the internet the speed of the internet must distribute equally among all the applications and websites. That is while accessing any website user does not have to shell out extra amount for extra speed for any particular website or application.

The debate of Net Neutrality sparked in India when the nation's largest telecom giant came up with a service called 'Airtel Zero' where customers of Airtel could access certain mobile applications for free of cost (Sharma 2015). However, the private companies including the start ups were made to incur the cost of the internet used by the mobile customers. This was announced at a time when Facebook and Reliance launched a program in India called 'Internet.org' which promised internet for all parts of India. This move by Airtel was heavily opposed by the people as it was against the concept of internet neutrality. The people started a massive movement on the internet with the popular hashtags like #savetheinternet. The people were mobilised regarding the subject from every means of internet communication. YouTube videos, hashtags in Facebook and twitter, emails, blogs were the media which people used to discuss and understand the issue. One of the important concerns were from the entrepreneurs. Already constrained by limited finance they would have to pay extra amount to take their website or web based application to the masses.

However, as far as regulation of such issues are concerned, there are no specific law concerning net neutrality in India.

The highest authority in regard to such issues is Telecom Regulatory Authority of India (TRAI) and it asked views from the people on net neutrality. Finally Airtel pulled back its initiative of zero marketing under pressure from the people. It was perhaps for the first time in India that a public debate on net neutrality was taking place between the state, Capitalist and people on such a large scale.

In the midst of such debate, apprehending similar fate, Facebook quietly changed the name of its project ‘Internet.org’ to ‘Free Basic’. Under ‘Free Basic’ all the mobile handset with Reliance India connection can access to a certain group of websites without any charge. That is the internet access will be provided to everyone with Reliance connection but only in a limited way. And one of the free website under this scheme is Facebook’s own website.

Facebook from its past experience in west and overall positive impact of connecting people, especially in mobilising for a common cause, was certainly confident about its project of ‘Internet.org’ in India. Revealing his intentions for the project, the founder of Facbeook Mark Zuckerberg said that he wanted to connect the people of India without Internet connect to the cyberspace so that it can provide ‘basic services for health , education , jobs and communication’ (Chaudhury 2016). This understanding of connecting the unprivileged India with the rest of India by Zuckerberg was not as straight as it sounds. Many people like bloggers, professors, students, activists, internet experts, and policy makers raised concerns over the true intention of Zuckerberg’s true intentions behind his ‘Free Basics’ (Chaudury 2016).

The major concern regarding the scheme was how feasible it was for the rural parts of India to access so called ‘basic’ services for health, jobs, and communication when there are so many constraints, owing to diversity in India, which makes it seemingly difficult to implement such one jacket plan for all. For instance, most of the websites covered under the scheme are in English language whereas the target audience of ‘Free Basics’ have no exposure to English because most of the people are educated in their local language and dialects. This ignorance of India’s local and rural languages clearly contradicts the initial objective of the scheme shared by Facebook (Chaudhury 2016).

Another important concern was that ‘Internet.org’ was clearly violating net neutrality as the service was providing limited internet access to the rural and remote parts of India. Many people and internet activist started the slogan of ‘poor internet for poor people’ (Chaudhury 2016).

In September 2015, among the midst of such opposition from the people across India and the debate over net neutrality Facebook quietly changed the name of Internet.org to ‘Free Basics’. In a progressive response over this TRAI announced that it would seek public and private stake holder’s opinion on the issue to decide the fate of ‘Free Basics’ in India. For almost a month TRAI started receiving opinions and views from the people, and businesses in the state to understand the stand of the people on the issue.

Appalled by such a mass movement against ‘Free Basics’ Zuckerberg immediately started reaching out to the masses of India through various channels like blogs, newspapers and other mediums. He plead India not to judge Free Basics and extend support to the scheme as it was meant for the progress of India as a whole and asked people to support its cause and help TRAI allow the implementing of the project.

When he realised that people were still unmoved towards their stand on the issue he went on to showcase something which India has never experienced before. Taking advantage of good number of Indian’s presence in Facebook he started notifying the users that their friends had signed online letter to TRAI in favour of Free Basics. At the same time full front page advertisement about the Free Basic started coming up in the most popular newspapers like Times of India, The Hindu, etc. These advertisements had the words like ‘Support a connected India. First step towards digital equality’ (Chaudhury 2016). Facebook spent about Rs. 300 crores in the print media on the advertisement about Free Basics (Vidhi Choudhary 2016). Later Facebook was also accused of misinforming people about the entire project. Finally after receiving inputs from the people and business, TRAI put ban on Free Basics and it marked a historic event of people over colonialist attempt to conquer the cyberspace in India by Facebook.

The move by TRAI to securitise cyberspace from the referent subject of ‘Airtel Zero’ and ‘Free Basic’s is truly a breakthrough in the decision making process of state. This marks a positive change in India’s decision making process.

Despite the already strong presence and good reputation of Facebook over the world, India chose not to bow before this US based company and strongly guarded the rural and poor Indians from exploitation. The entire process is emancipatory as firstly, the people voicing against Free Basics felt completely empowered and fearless in challenging the multi nationals like Airtel and Facebook. Secondly, there was a fine communication and cooperation between the people of the state and state. Both individuals and state, often looked as opposing forces, came together using social media and technology and worked in tandem with each other to arrive at the final decision.

Chapter 5

CONCLUSION

At the beginning of the dissertation, two hypotheses were proposed to address the research questions. The first, ‘Securitisation of cyberspace results in suppression of voices of the unheard in the international society’, and the second ‘inclusivity in cyberspace is leading to exclusivity of the marginalised’. Towards the end of research, the findings are in line with both the hypotheses. However, for the second hypothesis,a variable ‘globalisation’ is found to be an intervening variable.

Understanding securitisation from the consequentialist lens, this paper reached the conclusion that securitisation of cyberspace indeed results in suppression of the voices of the unheard. Due to the dynamic nature of cyberspace along with change in Information Technology and Communication (ICT) there has been a rise is growth of cyber crimes worldwide. In response to such attacks in cyberspace, states are investing heavily securitising this virtual space. There is an alarming trend that this effort of securitising cyberspace is leaning more towards military use than actually protecting and securing cyberspace.

The most advanced states in militarising cyberspace are the United States, China, Russia, Israel and the United Kingdom followed by emerging cyberpower states such as Iran and North Korea. Leading in the race is the United states. Post 11 September 2001, the Government of United States successfully made cybersecurity as its one of the top national security agendas, addressing the agenda of cybersecurity form a top-down approach. Establishment of USCYBERCOM in 2009 under the US Department of Defence is the epitome of this development. This is a shift from defensive to offensive stance in cybersecurity policy. Responding to this development, both Russia and China are now gearing up for an offensive stance. This stance by these states makes the space for insecurity than security. As a result, today cybersecurity policy documents and doctrines of these states are flooded with the words such as *cyberdeterrence*, *cyberwar*, *cyberdefense*, *cyberpower*, etc. Eventually, exploiting the cyberspace, which would otherwise have the potential to bringing the world together and closer to each other, ends up dividing and disconnecting the world even further.

This state centered centric of securitising cyberspace is certainly detrimental to the individuals and citizens of international society. Instead of directing the state's capacity and resources against the cybercriminals, states are deliberately suppressing freedom of expression of the voiceless and blocking information access to the masses. States such as China, UAE, and Bangladesh are few examples where the voices and concerns of individuals from marginalised sections are silenced and controlled by securitising cyberspace.

Analysing securitisation as a negative phenomenon, there is certainly enough evidence that with securitisation of cyberspace, the concerns and voices of the marginalised sections of international society are deeply suppressed. States, as securitising actors, are absolutely callous about the freedom of expression and basic rights of relating to accessing information from the vantage of the marginalised sections of the society. However, if securitisation is taken as a positive phenomenon (or *emancipatory securitisation*), then it is not difficult to see hope and optimism even in the present crackdown on individuals and societies or any other system by the existing governments of the various states. It is important to assert that this hope and optimism is not just an idealist thought. Rather it is evident from the networked social movements that an individual from a marginalised and fringed section of a society can turn the things around.

For instance, the '#YoSoy132' moment in Mexico City which exposed the nexus between state and television giant to misinform people is a great achievement for the powerless students. These students in relation to the state are always on the fringes as far the national policies or decision making is concerned. The 'Tahir Square' movement in Egypt is no different story. The individuals as a citizen of the state were totally frustrated with the government's apathy towards the welfare and growth of the people. Rather the state was promoting police brutalities and violence against the masses. In reaction to this, the internet connection to the entire state was cut-off. This further gave momentum to the protest and finally Mubarak had to resign from his office. In a completely historic moment in Indian history, for the first time, the state sought public opinion over the implementation of Facebook's project called 'Free Basics'.

After receiving all the comments and suggestions from the people, the state declined any permission to Facebook for the project. These victories of emancipatory securitisation by collective efforts of individuals over the state and multinational giant Facebook are clearly a positive move towards emancipation.

The findings also were in line with the second hypothesis that ‘inclusivity in cyberspace is leading to exclusivity of the marginalised’. The unquestioned growth of digitalisation around the world to include everyone and everything in cyberspace is indeed creating a major exclusion of the marginalised sections of society. For instance Facebook today is something which is almost universal as far as cyberspace is concerned. Even the government officials and leaders have presence in the social media. Being known for its supportive stand for social issues, Facebook fails to provide third option for gender while signing up with the social network site. One can only choose between ‘male’ and ‘female’ as gender. This is an example of exclusion of Lesbian Gay, Bisexual, Transgender and Intersex (LGBTI) from the social network site. Further an intervening variable ‘globalisation’ is found between the variables ‘inclusivity in cyberspace’ and ‘exclusivity of marginalised’.

Digitalisation today is a global phenomenon, a movement propagated by the states and private multi-national organisations. This forces individuals to follow certain standard practices as imposed and dictated by the rule of the digitalised world.

In case of states such as India, it is extremely difficult to digitalise every interface between the people and the government due to diverse socio-cultural composition of the population. In fact, many communities and tribes in India have their own language and dialect. The present numbers are 22 major languages with about 720 dialects. This inclusion process in cyberspace would definitely exclude a good number of tribal and marginal people at least for a reasonable period of time. Also, there could be certain communities or groups which may not be comfortable to expose themselves to the digital world.

Further there is scope for research on the definition of ‘emancipatory securitisation’ and how it can contribute to inclusion of the marginalised. In other words, how this could emancipate not only the individual but all the marginalised sections of a society, community or international society needs to be explored.

Also, the intervening variable ‘globalisation’ can be further studied thoroughly in order to address the following questions: What is it about globalisation that contributes to the exclusion of marginalised?

References

Alden, C. (2003), “Let Them Eat Cyberspace: Africa, the G8 and the digital divide”, *Millennium: Journal of International Studies*, 32(3): 457-476.

Al-Mahmood, S. Z. (2016), “Hackers lurked in Bangladesh Central Bank’s servers for weeks”, [Online: web] Accessed 9 July 2016, URL: http://www.wsj.com/articles/hackers-in-bangladesh-bank-account-heist-part-of-larger-breach-1458582678.

Amnesty International. (n.d.), “Freedom of Expression and the Internet”, [Online: web] Accessed 12 June 2016, URL: http://www.amnestyusa.org/our-work/issues/censorship-and-free-speech/internet-censorship.

Anand, V. (2006), “Chinese Concepts and Capabilities of Information Warfare”, *Strategic Analysis*, 30 (4): 781-797.

Balzacq, T. (2011), “A Theory of Securitisation: Origin, core assumptions, and variants”, in Thierry Balzacq (eds.) *Securitisation Theory: How security problems emerge and dissolve*, New York: Routledge .

Baker, E. W. (2014), “A Model for the Impact of Cybersecurity Infrastructure on Economic Development in Emerging Economies: Evaluating the Contrasting Cases of India and Pakistan”, *Information Technology for Development*, 20 (2): 122-139.

Booth, K. (1991), “Security and Emancipation”, *Review of International Studies*, 17(4): 313-326.

Booth, K. (2007), *Theory of World Security*, New York: Cambridge University Press.

Branigan, T. (2012). “China cut off internet in area of Tibetan unrest”, [Online: web] Accessed 12 March 2016, URL: https://www.theguardian.com/world/2012/feb/03/china-internet-links-tibetan-unrest.

Breene, K. (2016). “Who are the cyberwar superpowers?”, [Online: web] Accessed 11 July 2016, URL: https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers

Brown, C. (2013), “The poverty of Grand Theory”, European *Journal of International Relations*, 19(3): 483-497.

Buzan, B. et al. (1998). *Security: A new framework for analysis*, London: Lynne Rienner.

Carr, M. (2015), "Power Plays in Global Internet Governance", *Millennium: Journal of International Studies*, 43(2): 640-659.

Caudhury, M.R. (2016), "Spotlight on India's Internet: Facebook's Free Basics or Basic Failure?", [Online: web] Accessed 2 March 2016 URL: https://jsis.washington.edu/news/spotlight-indias-internet-facebooks-free-basics-basic-failure.

Caudhury, V. (2016), "Facebook spends around Rs300 crore on Free Basics ad campaign in India", [Online: web] Accessed 24 June 2016 URL: http://www.livemint.com/Consumer/oMmTd2g4CkwErMNRoedVMJ/Facebook-spends-around-Rs300-crore-on-Free-Basics-ad-campaig.html

Cavelty, M. D. (2014), "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities", *Science & Engineering Ethics*, 701-715.

Cattle, A.E. (2016), "Digital Tahrir Square: An Analysis of Human Rights And The Internet Examined Through The Lens Of The Egyptian Arab Spring", *Duke Journal of Comparative & International Law*, 2(26), 418-449.

Chow, L. (2015), "Leonardo DiCaprio: 'We Are the Last Generation That Has a Chance to Stop Climate Change'', [Online: web] Accessed 23 March 2016, URL: http://www.ecowatch.com/leonardo-dicaprio-foundation-gala-raises-45-million-1935461575.html

CISCO. (2016), *Cisco 2016 Annual Security Report*. CISCO, United States of America

Dartnell, M (2003), "Weapons of Mass Instruction: Web Activism and the Transformation of Global Security", *Millennium: Journal of International Studies*, 32(3): 477-499.

Deibert, R.J. (2003), "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace", *Millennium: Journal of International Studies*, 32(3): 501-530.

Demidov, O. (2013), "Cyberwarfare and Russian Style Of Cyberdefense", *Security Index* , 19: 67-71.

Diskaya, A. (2013). "Towards a Critical Securitization Theory: The Copenhagen and Aberystwyth Schools of Security Studies", [Online: web] Accessed 10 April 2016, URL: http://www.e-ir.info/2013/02/01/towards-a-critical-securitization-theory-the-copenhagen-and-aberystwyth-schools-of-security-studies/

Dreher, A et al. (2008), *Measuring Globalisation: Gauging its Consequences*, New York, United States: Springer.

Floyd, R. (2007), "Towards a consequentialist evaluation of security: bringing together the Copenhagen and the Welsh Schools of security studies", *Review of International Studies*, 33 (2): 327-350.

Freedom House. (2015). *Privatizing Censorship, Eroding Privacy*: Freedom on Net 2015. Freedom House.

The Guardian (n.d.), "Australian miners fired for 'Harlem Shake'", [Online: web] Accessed 10 April 2016, URL: https://www.theguardian.com/business/2013/mar/04/harlem-shake-australian-miners

Global Research and Analysis Team (2013), Kaspersky Lab. [Online: web] Accessed 11 June 2016, URL: https://securelist.com: https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation

Globalizing Cyberspaces. (n.d.). [Online: web] Accessed 12 June 2016, URL: culturalpolitics.net: http://culturalpolitics.net/digital_cultures/global

Guitton, C. (2013), "Cyber insecurity as a national threat: overreaction from Germany, France and the UK?", European *Security*, 22 (1): 21-35.

Hansen, L. (2000). The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School. *Millennium: Journal of International Studies*, 29 (2), 285-306.

Hansen, L. (2009), "Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly*, 53: 1155-1175.

Harknett, R. J and Stever, J. A. (2009), "The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen", *Journal of Homeland Security and Emergency Management* , 6 (1).

Harris, S. (2015), "China Reveals Its Cyberwar Secrets", [Online: web] Accessed 12 June 2016 URL: http://www.thedailybeast.com/articles/2015/03/18/china-reveals-its-cyber-war-secrets.html.

Hindustan Times Correspondent (2015), "Facebook trouble: 10 cases of arrests under Sec 66A of IT Act", [Online: web] Accessed 23 October 2016, URL: http://www.hindustantimes.com/: http://www.hindustantimes.com/india/facebook-trouble-10-cases-of-arrests-under-sec-66a-of-it-act/story-4xKp9EJjR6YoyrC2rUUMDN.html

Hjalmarsson, O. (2013). "The Securitization of Cyberspace: How the Web Was Won", [Online: web] Accessed 23 March 2016, URL: https://lup.lub.lu.se/student-papers/search/publication/3357990

Hollis, D. M. (2010), "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command", *Joint Force Quarterly*, 3 (58): 48-53.

Homeland Security (2016). "National Protection and Programs Directorate", [Online: web] Accessed 14 June 2016, URL: https://www.dhs.gov/national-protection-and-programs-directorate.

Houser, W. (2015), "Could What Happened to Sony Happen to Us?" *IT Professional* , 17 (2): 54-57.

International Telecommunication Union (2015), *Measuring Information Society Report 2015,* Switzerland.

John Fien. (n.d.). "Globalisation", [Online: web] Accessed 10 March 2016, 2016 URL: http://www.unesco.org/: http://www.unesco.org/education/tlsf/mods/theme_c/mod18.html

Kabin, B. (2013, September 11). Apple's iPhone: Designed in California But Manufactured Fast All Around the World (Infographic). [Online: web] Accessed 23 April 2016, URL: www.entrepreneur.com: https://www.entrepreneur.com/article/228315

Kavanagh, C. (2014), “Introduction to Special Issue: Cybersecurity, Sovereignty, and U.S. Foreign Policy ”. *American Foreign Policy Interests*, 36 (5): 283-285.

Kaspersky Lab (2015). *Carbanak APT: The Great Bank Robbery*. Kaspersky.

Khadekar, N. (2015), “What is net neutrality and why it is important in India”, [Online: web] Accessed 10 January 2016, URL: http://tech.firstpost.com/news-analysis/what-is-net-neutrality-and-why-it-is-important-in-india-262120.html

Kremera, J. (2014). “Policing cybercrime or militarizing cybersecurity? Sescurity mindsets and the regulation of threats from cyberspace”. *Information & Communications Technology Law*, 23 (3): 220-237.

Liaropoulos, A. (2013), *Exercising State Sovereignty in Cyberspace: An International Cyber Order Under Construction?* Proceedings of the8th International Conference on Information Warfare and Security, 136-140, Colorado.

Libicki, M. C. (2009), *Cyberdeterrence and Cyberwar*, RAND Corporation.

Losh, S. C. (2010), “Generation, Education,Gender, and Ethnicity in American Digital Divides”, in E. F. Dwivedi, J. R. Gil-Garcia, and M. D. Williams (eds.), Overcoming Digital Divides, 196-221, Hershey: *Information Science Reference*.

Mclnnes, C., and Rushton, S. (2011), “HIV/AIDS and Securitization Theory”, European Journal of International Relations , 19 (1).

Mizor, P. (2015). “China Cuts Mobile Service of Xinjiang Residents Evading Internet Filters”, [Online: web] Accessed 9 March 2016, URL: http://www.nytimes.com/2015/11/24/business/international/china-cuts-mobile-service-of-xinjiang-residents-evading-internet-filters.html?_r=0

Mooney, A., and Evans, B. (2007). *Globalisation: The Key Concepts. London*: New York: Routledge .

Mozur, P. (2016). “Beijing Seeks to Tighten Reins on Websites in China”, [Online: web] Accessed 9 July 2016, URL: http://www.nytimes.com/2016/03/30/technology/china-internet-censorship.html?rref=collection%2Ftimestopic%2FInternet%20Censorship%20in%20China&action=click&contentCollection=world&region=stream&module=stream_unit&version=latest&contentPlacement=6&pgtype=co.

Mulvenon, J. (1999), “The PLA and Information War “ in James C. Mulvenon, Richard H. Yang (eds.), *The People's Liberation Army in the Information Age*, RAND Corporation.

NATO Review (n.d.), “The History of Cyber Attacks - a timeline”, [Online: web] Accessed 11 June 2016, URL: http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm.

Nye, J. S. (2011), “Nuclear Lessons for Cyber Security?”, *Strategic Studies Quarterly* , 18-38.

Nye, J. S. (2012), “Cyberwar and Peace”, [Online: web] Accessed 10 April 2016, URL: http://www.project-syndicate.org/commentary/cyber-war-and-peace

Oxford English Dictionary, (2012). *Oxford English Dictionary*, Oxford, United Kingdom: Oxford university press.

Press Trust of India (2016), “China defends crackdown against Islamic militants in Xinjiang”, [Online: web] Accessed 12 July 2016, URL: http://economictimes.indiatimes.com/: China's Brutal Crackdown in Xinjiang.

Press Trust of India (2012), “Two Mumbai girls arrested for Facebook post against Bal Thackeray get bail”. [Online: web] Accessed 11 April 2016, URL: http://indiatoday.intoday.in/: http://indiatoday.intoday.in/story/2-mumbai-girls-in-jail-for-tweet-against-bal-thackeray/1/229846.html.

Purnell, N. (2016), “Facebook Receives Highest-Ever Number of Requests for Indian User Data”, [Online: web] Accessed 22 March 2016, URL: http://blogs.wsj.com/: http://blogs.wsj.com/indiarealtime/2016/04/29/facebook-receives-highest-ever-number-of-requests-for-indian-user-data.

Roney, T. (2013), “China's Brutal Crackdown in Xinjiang”, [Online: web] Accessed 12 July 2016, URL: http://thediplomat.com/2013/10/chinas-brutal-crackdown-in-xinjiang.

Rushe, D. (2015), “The Interview revenge hack cost Sony just $15m”, [Online: web] Accessed 11 July 2016, URL: https://www.theguardian.com/film/2015/feb/04/guardians-peace-revenge-hack-sony-finances-unscathed

Sanger, D. E. (2016), "U.S. Cyberattacks Target ISIS in a New Line of Combat", [Online: web] Accessed 12 June 2016 URL: http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=0

Segev, E. (2010), *Google and the Digital Divide: The bias of online knowledge.* Oxford, United States: Chandos Publishing.

Selwyn, N., and Facer, K. (2010), "Beyond Digital Divide:Toward an Agenda for Change", in E. Ferro, Y. K. Dwivedi, J. R. Gil-Garcia, M. D. Williams, E. Ferro, Y. K. Dwivedi, J. R. Gil-Garcia, & M. D. Williams (eds.), *Overcoming Digital Divides United States,* Information science reference.

Sharma, S. (2014), "Airtel Zero Stirs Net Neutrality Debate with New 'Toll-Free' Marketing Platform", [Online: web] Accessed 4 May 2017, URL: http://www.huffingtonpost.in/2015/04/07/airtel-zero-stirs-net-neutrality-debate-with-new-toll-free-mar/?utm_hp_ref=in-net-neutrality-india

Shi, T., and Zhai, K. (2015). "China Military Seeks to Bring Cyber Warfare Units Under One Roof", [Online: web] Accessed 12 May 2016, URL: http://www.bloomberg.com/news/articles/2015-10-22/china-military-chiefs-seek-to-unify-cyber-warfare-operations

Stritzel, H. (2007), "Towards a Theory of Securitization:Copenhagen and Beyond", *European Journal of International Relations,* 13 (3).

Treré, E. (2015), "Reclaiming, proclaiming, and maintaining collective identity in the #YoSoy132 movement in Mexico: an examination of digital frontstage and backstage activism through social media and instant messaging platforms", *Information, Communication & Society,* 8(18): 901-915

Tuner, E. (2013), "New Movements, Digital Revolution and Social Movement Theory", *Peace Review,* 3(25): 376-383.

Waddell, K. (2015), "Why Google Quit China—and Why It's Heading Back", [Online: web] Accessed 21 April 2016, URL: http://www.theatlantic.com/technology/archive/2016/01/why-google-quit-china-and-why-its-heading-back/424482.

Watson, S. (2011). “The ‘human’ as referent object? Humanitarianism as securitization”, *Security Dialogue,* 3-20.

Warschauer, M. (2003), *Technology and Social Inclusion: Rethinking the Digital,* Massachusetts, United States: MIT Press.

Weber, R. H., and Heinrich, U. I. (2012), *Anonymization*, Springer.

Western, S. (2014), “Autonomist leadership in leaderless movements: anarchists leading the way”, *Ephemera*, 4(14), 673-698.

Wikipedia. (n.d.). “Websites blocked in mainland China”, [Online: web] Accessed 12 May 2016, URL: https://en.wikipedia.org: https://en.wikipedia.org/wiki/Websites_blocked_in_mainland_China.

Williams, M. C. (2003), “Words, Images, Enemies: Securitization and International Politics”, *International Studies Quarterly*, 47: 511-531.