Knowledge is Power: The Internet Panopticon as a Weapon against Terror

https://www.e-ir.info/2016/05/19/knowledge-is-power-the-internet-panopticon-as-a-weapon-against-terror/

RUDHAYAINI VIJAY MUKANE, MAY 19 2016

CHAPTER ONE: Introduction

The immense developments in information and communication technologies (ICTs) have radicalized the ways in which societies operate in the modern era. There is an increasing societal dependence on ICTs on various levels, which has transformed the ways in which the individuals and even states interact with each other at the private, public, national or international level. For example, digital infrastructures: encourage economic development and transnational research; strengthen military and defense systems; make governments transparent and support an open society. Today there are over 3.2 billion internet users in the world, accessing over 920 million websites, sending 210 billion emails daily and conducting 4.2 billion Google searches at any given moment, and these numbers keep increasing at a rapid pace (internetlivestats.com, 2015). Although, a digital gap persists between the 'information rich' and 'poor', it remains undeniable that ICTs, especially the internet, have revolutionized commerce, communication, military action and governance (Knake, 2010; Radu, 2014:5). The modern world is inconceivable without these technologies and we will continue to become increasingly dependent on these networked information systems. Overall, it can be said that digital technology and computers have become ubiquitous in all aspects of human life.

The aforementioned digital revolution has led to the emergence of cyberspace. Cyberspace can be understood as a metaphor describing a non-physical terrain created by the international network of computers (Awan and Blakemore, 2012:5). Fundamentally, cyberspace is real, as it is physically constructed through network information technology. But it is also a social construction shaped by discourses that people and institutions produce, which has its own systems of social relations formed by the heterogeneous participants and netizens (Barnard-Wills and Ashenden, 2012:111).

Some argue that this cyberspace is redefining our postmodern society on many levels, political, social and economic and changing the relations between states, people and corporations, due to its liberating yet confining nature (Lessig, 2006). Preston C. Russett takes a negative stance with regards to cyberspace and argues that it creates a space where it is impossible to not leave behind any trace, hence eliminating any scope for privacy. Additionally, he argues that "the digital data-filled sludge people smudge across the cyber spheres and upload into the world does not fade into an abyss but is harvested and hoarded for exploitation" (Russett, 2011:42). For example, corporations profit by surveying the routine behaviors of people online and continuously coding them to create digital profiles of people. This is enabled because people are increasingly relying on free softwares such as Google Maps or online banking to make real life more convenient. Accordingly, the Internet has its disadvantages.

Internet technologies also bring about many unknown and incalculable malicious threats in the form of cyber terrorism, cyber-attacks, cyber-warfare as is evident from the attacks on Estonia, Georgia and the Stuxnet virus

which trampled Iran's nuclear ambitions (Greathouse, 2014:22; Knake, 2010:6). Governments all over the world have realized the importance of cyberspace for maintaining their security, and a vast discourse is being produced highlighting the importance of cyber-security and securing cyberspace in light of the dual-nature of cyberspace (Renard, 2014:7). Especially following the terror attacks of 11th September 2001 (hereon 9/11), there has been a strong emphasis on not only securing cyberspace but also utilizing cyberspace capabilities to prevent future attacks (Knake, 2010; Radu, 2014:13).

The postmodern era, with its technological developments, has brought with it numerous vulnerabilities that must be tackled immediately. The previous, Cold War era provided a sense of certainty because threats to a state's security were mostly in the form of physical, quantifiable and direct military and economic capabilities that could be traced back to other states (Williams, 2008). In contrast, the cyber-era is being referred to as the 'age of uncertainty' in policy documents, as the new threats being faced by states emanate not just from states, but non-state actors such as homegrown or foreign terrorists, insurgents or criminals and other unknowable entities (Government of UK, 2010).

One of the major implications of these threats, especially 9/11 and the subsequent 'war on terror' has been the change of privacy and surveillance-policies in many countries of the West and even the East (Fuchs, Boersma, Albrechtslund and Sandoval, 2011:10). These changes in policies allow the state governments to intercept, collect, analyze and store internet and communications data on their own and even foreign citizens through mass surveillance programs. For instance, the 'USA PATRIOT ACT' passed in 2001, widened the scope of data (such as name, address, identity, services used, duration of calls made, content of emails, bank details) that the US government can now gain access to via internet service providers. Some have argued that while the digital age has made surveillance more opaque, the effects are equivalent to that of Jeremy Bentham's prison model of the all-seeing, all-disciplining Panopticon (Williams, 2015).

In light of the above developments, the aim of this dissertation is to critically assess the claim that we are now enclosed in a virtual Panopticon made possible by developments in cyberspace and reliance on the Internet, which is in turn used by states as a technology to govern the social problem of terrorism, through the precautionary *dispositif* of risk. It will be argued that the Internet, by virtue of its architecture functions as a Panopticon which is wielded by states and their governments through anti-terrorism legislations, as a precautionary technology to control and govern the risk of terrorism.

Firstly, this dissertation will analyze postmodern security practices by utilizing Ulrich Beck's framework of 'world risk society' to investigate the changing nature of threats, and will examine the features of new terrorism that transform it into a risk. Secondly, it will be argued that this risk of terrorism, because of its uncertain, unknowable, and possibly catastrophic nature brought upon by technological developments, becomes a social problem that must be governed. Using Michel Foucault's governmentality thesis, this dissertation will develop the risk of terrorism as a precautionary *dispositif*, which transforms terrorism into a problem that can only be controlled by gathering knowledge. Thus, Governments become obsessed with total information access, which legitimizes extensive surveillance practices as everyone is a suspect. It will be demonstrated that, in this quest of knowledge and control, the Internet and its wide-reaching surveillance potential is an important tool for states in the fight against terror. In sum, this dissertation will analyze how the Internet, functions as a Panopticon which is used by states as a precautionary *dispositif* to deal with terrorism. Finally, the societal resistances to this phenomenon and their implications will be examined.

CHAPTER TWO: The Risk-Counterterrorism-Surveillance Nexus

Security is a concept that has evolved over time. Hence, it remains a contested term not only in academia, but also in international relations (Diez, Bode and da Costa, 2011:193). Historically, security meant protecting the territorial integrity and polity of a state from other states, fundamentally through military capabilities. Although security policies

were closely linked to defense policies, they entailed broader foreign policy aspects such as cooperation through the UN as an alternate to military means for ensuring the state survival (ibid).

However, following the terror attacks of 9/11, the definition of security in international relations has changed dramatically from its original definition. Aradau and van Munster have aptly described that the 'war on terror' has now brought on practices which fall beyond the purview of war, such as "Guantanamo Bay to biometrics and increased surveillance, or from extraordinary rendition to the categorization of terrorist suspects as enemy combatants," (Aradau and Munster, 2007:90). These changes have been brought about by not only a quantitative increase in the number of perceived threats the state faces, but also the change in their interpreting of danger as 'risks' instead of threats.

The following section will explain the concept of 'risk' in contemporary society, and how 'terrorism' as a risk, both in real space and 'cyberspace', comes to define the new security practices of states.

World Risk Society and Obsession with Securing Against Risks

Despite high levels of scholarly contributions to the subject, no perfect definition of 'risk' exists. Yee-Kuang Heng provides a useful description: risk can mean a "descriptive term referring to a potentially dangerous situation; or it can also be normative, implying the desire for anticipatory avoiding action as part of a proactive risk calculation" (Heng, 2006:71). The term 'risk' as a policy concept can be traced to the end of the Cold War, when major states and international organizations began to describe their security environment in terms of risk rather than dangers (Aradau, Lobo-Guerrero and Munster, 2008).

However, the events of 9/11 brought Ulrich Beck's 'world risk society' thesis into the focus of security studies. Beck theorized that risks in contemporary society are an issue for security due to their unique temporal and spatial mobility as globalization makes risks transcend territorial boundaries and difficult to locate in time (Beck and Lash, 1992). Not only are these risks delimited spatially and temporally, but they are also socially de-bounded, because they affect everyone no matter their social class. This de-boundedness creates potential for great societal harm and generates irremediable effects. Moreover, the destructive force of these risks makes it impossible to insure against them.

Beck's conceptualization of the world risk society argues that the effects of modernization produces a "gulf between the world of quantifiable risk in which we think and act, and the world of non-quantifiable insecurities that we are creating" (Beck, 2002:40). Risks in the industrial age in the 20th century were understood as side effects of industrialization affecting only the individual; they could be calculated, tamed and insured against. But the new risks that emerge from unprecedented technological and industrial advancements are ultimately unpredictable, uncontrollable and indescribable risks affecting on a global scale (Aradau and Munster, 2007; Heng, 2006).

Thus, the world risk society is reflexive in nature, as the risks are consequences of the threatening force of modernization (Beck and Lash, 1992:21). Unlike the previous dangers which were externally produced insecurity subjects, risks originate from our own actions (Rasmussen, 2004:393). Beck's concept of risk, superimposes the present with the future, because the actions and decisions in the present can lead to potentially dangerous consequences in the future. The 'world risk society' is a future-facing society due to an obsession with speculating about all possible futures, as opposed to the industrial society where risks could be calculated based on past experiences (Clapton, 2009).

This language of risk is hard to miss in the security strategies and policies states pursue, especially Western societies such as the US. There is evidence of this in the successive administrations of Clinton, Bush and Obama (Clapton, 2011). Similar to Beck, the 2015 US National Security Strategy cites "violent extremism and an evolving terrorist threat" as a persistent, anxiety and insecurity inducing risk to American and global security, along with the "escalating challenges to cybersecurity, the accelerating impacts of climate change and the outbreak of infectious diseases" (The White House, 2015).

Beck's world risk society thesis helps explain how terrorism serves as a classic world risk society problem. Terrorist

networks have an international reach and global presence, as is evident by the various attacks carried out by Al-Qaeda in places like London, Madrid, New York that span the past two decades (Google, 2015). Moreover, developments in ICTs and the advent of the internet allow terrorism to permeate and operate through cyberspace. Terrorist networks use these technologies not only to forward their propaganda, but also plan and execute attacks which damage both virtual and actual spheres of life (Westby, 2006). The risk of terrorism, is de-bounded temporally and spatially through technological developments, and the dominant policy narratives of the states like the US (as seen above) reinforce it as a globally universal threat capable of affecting everyone due to the interconnected nature of our networked societies (NATO Review, 2015; Mythen and Walklate, 2008).

Moreover, the same technological advancements that benefit society can provide terrorist groups with numerous modes of attack such as remotely activated explosives (in the 2004 Madrid attacks, bombs were set off using mobile phones), or the ability to hack into systems causing failure of critical infrastructure, having catastrophic consequences (Beck, 2002). The risk of terrorism thus becomes uninsurable through the uncertainty of its nature, location and the difficulty to perform risk assessments.

Beck's 'world risk society' theory helps us understand the transition into a postmodern, global risk society which is categorized by temporally, spatially and socially de-bounded risks (Clapton, 2011). But this dissertation takes issue with his claims that these 'risks' are unquantifiable, uninsurable, unknowable and uncontrollable, as they fall short in explaining the risk management and analysis practices undertaken by states. Furthermore, his conceptualization does not help us understand whether there are objective, real risks out there (Heng, 2006).

Some critics of Beck have argued that risks are constructed through the security discourses of dominant institutions, shaping our understanding and recognition of certain phenomenon as "risks" (O'Malley, 2009). However, it can be argued that risks are in fact performative; they cannot be isolated as tangible because they produce the effects they name (Amoore and Goede, 2008). It is beyond the scope of this essay to verify the objectiveness of risks, but Aradau and van Munster's 'precautionary risk' concept provides a better understanding into the current practices undertaken by states to govern these security risks, specifically terrorism. This concept helps us understand how the Internet Panopticon is enabled to take precautions against terrorism.

Terrorism Risk: A Tale of Precaution

Beck's core claim is that, decision-makers can no longer guarantee predictability, security and control when faced with conditions that are indeterminate in the risk society. Thus, the main concern is "how to *feign* control over the uncontrollable" (Beck, 2002:41, emphasis added). Control becomes a fantasy, something that one can only pretend to achieve, but ultimately it remains beyond reach. Similarly, Rasmussen too claims that when faced with a risk such as terrorism, the notion of complete security is unfeasible and hence the focus is shifted to "managing" these risks in uncertain conditions (Rasmussen, 2004).

However, the issue with these arguments of 'risk' as unknowable and unmeasurable, hence uncontrollable, divert attention from the fact that the global war on terror displays an 'insatiable quest for knowledge and control' which is observable in the security practices of profiling populations, surveillance, intelligence-gathering, the knowledge about catastrophe management and the precautionary approach to risk (Aradau and Munster, 2007, p.91). In light of these developments in security practices post-9/11, it is important to consider a different conceptualization of risk as a *dispositif* to govern social problems. Michel Foucault's 'governmentality' approach helps us understand how states seek to control the future through the discourse and technologies of risk (Mythen and Walklate, 2008).

Governmentality is the combination of 'governing' and modes of thought ('mentality'), entailing the study of technologies of power and the rationalities that underpin them (Lemke, 2002). Governmentality is, simply, the "conduct of conducts" (Burchell, Gordon and Miller, 1991:2). The practices of government function by constituting power relations between the one governing and the ones being governed. Power here functions through subtle coercion and influencing persons to behave in particularly desired ways (Foucault, 1991). Government, according to Foucault, "is the right disposition of things, so as to reach a convenient end" (Foucault, 1991:93). The right disposition of things entails employing tactics instead of laws and sometimes even laws are used as tactics

(Foucault, 1991:95).

These tactics can be understood as *dispositifs,* consisting of heterogeneous devices including "discourses, institutions, architectural forms, regulatory decisions, laws, administrative measures, scientific statements", serving as the rationalities and technologies of government (Aradau and Munster, 2007:97). Here, rationalities are certain ways of thinking about social problems that allow managing them and technologies are the means to realize these rationalities (ibid). Thus, Aradau and van Munster argue that it becomes necessary to analyze risk as a governing principle through which social problems such as terrorism are managed (Aradau and Munster, 2007).

Risk becomes a combination of these rationalities and technologies, comprising of calculations in the present to gauge future outcomes and employing certain devices in the present to try to control that potential future. This new *dispositif* of risk has at its core the principle of precaution, whereby uncertain threats, which cannot be scientifically calculated or proven and could lead to irreversible or serious damage, need to be prevented. Guldberg argues that this precautionary principle demands *unmanageable* risks be dealt with "not on the basis of what we know, but on the basis of what we do not know" (Guldberg, 2003). Terrorism, fueled by technological innovations in the cyber age, thus becomes a 'risk beyond risk' which Beck aptly describes as being unknowable and unmeasurable. But it is the precautionary *dispositif* of risk that aims to make terrorism governable. Take for example, the various criminal network analysis systems used by the governments of the USA, Germany, India and the UK to prevent terrorism by collecting and analyzing multimedia data dredged from ICTs. They utilize tools such as Counter-Terror Social Network Analysis and Intent Recognition (CT-SNAIR) and Terrorist Action Description Language (TADL) in order to not only detect and track terrorists groups and their intents, but also to simulate and statistically model terrorist networks and attacks (Weinstein, Campbell, Delaney and O'Leary, 2009; Wyld et al., 2011). This demonstrates that governments rely on the precautionary principle to govern the risk of terrorism before it even has a potential to materialize.

The precautionary *dispositif* of risk, is central to this dissertation, because it focuses on *how* to control the disastrous risk of terrorism by birthing new rationalities of government and utilizing existing technologies in new ways to tame and manage the future (Amoore and Goede, 2008). Following 9/11, Stewart Baker from the Department of Homeland Security remarked that 9/11 could have been prevented if better systems had been put in place allowing access to more data for creating a bigger picture of probabilities by connecting the information gained from multiple sources (Baker, 2006). This birthed the rationale behind, and political support for, increased knowledge gathering and analyzing technologies to be used in the management of terrorism. Furthermore, because terrorism is a risk that stems from lack of knowledge, the technologies utilized to govern terrorism become more extensive, general and applied to everyone (Aradau and Munster, 2007). This is evident in the shift from targeted profiling and surveillance as a means of preventing the catastrophe of terrorism, to mass surveillance (Rotenberg, Scott and Horwitz, 2015). The precautionary *dispositif* of the terrorist risk enlarges the scope and field of knowledge and intelligence gathering due to the uncertainty that the suspect could be anyone. This trend of the 'insatiable quest of knowledge' in order to govern the problem of terrorism is visible in legislations, such as the Foreign Intelligence Surveillance (FISA) Amendments Act (FAA) 2008 of the USA, the Telecommunications Act 1984 of the UK and the Telegraph Act 1885 of India as well as those of countries like France, Germany and Sweden (GPO, 2015; Government of India, 2015, Telecommunications Act 1984). Some commentators argue that such laws bring forth panoptic forms of surveillance that target everybody (see Chapter 3).

The precautionary *dispositif* of risk of terrorism also highlights the 'insatiable quest for control', (Mythen and Walklate, 2006). The precautionary devices which allow for gathering knowledge and knowing the unknowable also help mark out the boundaries of risk. With the risk of terrorism, everyone becomes a suspect that must be surveyed, but this surveillance works by preventing suspects from "acting" by classifying and separating the objects of surveillance into categories of risk (Mythen and Walklate, 2006; Lyon, 2013). Classification of populations based on their risk values serves as a deterministic technology of "pre-crime" control (O'Malley, 2009). The precautionary *dispositif* also subtly controls society by seeking to normalize and promote certain behaviors amongst populations (see next section). Furthermore, through an application of knowledge to the unknown and uncertain, there is an attempt to order or master this uncertainty, especially in the context of terrorism (Doty, 2015:345). Borrowing Ian Hacking's famous idea, "taming of chance", through the governmentality and *dispositif* of risk, states exhibit a desire

to control the future (Hacking, 1990). Through the linking together of knowledge, social control and classificatory techniques to control populations, "risk is operationalized as a mode of regulation, through which populations are surveyed" and control is obtained (Mythen and Walklate, 2006:385). Surveillance, which is made general and arbitrary, is used to expand the limits of knowledge and control and allows for governing terrorism through risk and its precautionary *dispositif* (Aradau and Munster, 2007:108).

Thus, the Foucauldian governmentality thesis helps us understand how the concept of risk with its multiple and heterogeneous practices, can be viewed under the purview of a precautionary *dispositif* and used to govern the social problem of terrorism. For these purposes, surveillance becomes an important technology to govern the risk of terrorism, because, the underlying principle of surveillance is that it allows for monitoring people and collecting information which can then be analyzed. The next section will describe in depth how surveillance is used as a precautionary technology to govern the risk of terrorism.

Knowledge is Power: Surveillance and Terrorism Control

Surveillance has historically been a feature of human societies (Lyon, 2006). For Realists, surveillance was a means of intelligence-gathering used by states in order to have an information edge over adversaries in a world where survival is the prime objective (Jensen, McElreath and Graves, 2013). But as Ayse Ceyhan describes, surveillance also functions as an apparatus '(*dispositif*) of security': a form of liberal governmentality used by states or powerful institutions/organizations to seek maximum efficiency by observing, classifying and sorting individuals in order to tackle uncertainties (Ceyhan, 2012:38).

A continuity of such uncertainty management via surveillance, is also visible following 9/11 as monitoring and identifying technologies have begun playing a central role in the public domain, majorly in the Western societies and many South-Asian countries due to the risk of transnational terrorism (Lakshman, 2015). Christian Fuchs provides an apt definition for surveillance in our contemporary society: "the collection of data on individuals or groups that are used so that control and discipline of behavior can be exercised by the threat of being targeted by violence" (Fuchs, 2011:136). With the rationale of counterterrorism, surveillance technologies are introduced increasingly and legitimized, while populations are disciplined to willingly accept these systems as the "price for security" (Lyon, 2003:675). This willingness is seen when surveillance technologies such as magnetic chip activated "smart" identity cards, biometrics, facial-recognition associated CCTV cameras and full-body scanners are unquestioningly accepted as a means for safety and security (ibid). Frank Furedi has described the furtive obsession with risk and security as creating a 'culture of fear', which is propagated by political discourses and is used to normalize surveillance practices (Furedi, 2002). It is also argued that this discourse and the surveillance systems help enhance state power (Lyon, 2003). Others have also contended that people are seduced into accepting and participating in their own surveillance due to the pleasures offered by consuming surveillance-accomplishing technologies such as the Internet and its enabling devices, rather than being forced into compliance by the threat of an authoritarian Big Brother (Lyon, 1994:75). This can be evidenced, for instance, when people participate in online surveys to win extra rewards in games like Candy Crush, thus willingly providing personal information to third-parties. Moreover, a unique allegiance between private corporations who have a vested, commercial interest in surveillance and state bodies wishing to control the risk of terrorism, is also visible post-9/11; thus redrawing power relations in the state-corporations-populations nexus (Lyon, 2003). This will be demonstrated in the next section.

Furthermore, the success these surveillance technologies have in stopping terrorism, and their effectiveness in predicting and preventing crime remains trivial compared to the profits of gaining total information. It is subtly understood that there are no total solutions to the threats and dangers of terrorism, they can only be managed, but not completely prevented (van Heuven, Botterman and De Spiegeleire, 2003). Therefore, surveillance systems are increasingly embedded in the architecture of our daily lives because gathering personal information on people; identification and data analysis become a core part of managing these unsolvable problems (Lyon and Haggerty, 2012). With the advent of ICTs and Internet enabled technologies, which have become ubiquitous in our daily lives, surveillance also becomes ubiquitous.

Internet surveillance is enabled by a multitude of methods for governments to pick and choose from, in order to

collect such vast quantities of communications. The most commonly used ones include tapping directly into (submarine) fiber-optic cables used for transmitting international communications, redirecting internet traffic via the repositories of SIGINT (signals intelligence) agencies as they traverse the country's systems (especially true in the case of the US as most of the worldwide communication traverses through there), cooperating with intelligence agencies in other countries and relying majorly on Internet companies, telecoms and ISPs to gain access to the data of their customers (Greenwald, 2014, p.101). Thus the Internet becomes an important technology to govern the risk of terrorism.

The changing features of surveillance post-9/11, enabled by the Internet can be understood better by analyzing the "dataveillance" capabilities of the Internet which allow systematic monitoring of people's actions or communications (Clarke, 1988, p.500). The architectural and technological nature of the Internet allows for perpetual capture of data on people, which resembles the Panopticon: a technology for mass surveillance. In order to understand how the Panopticon functions, this dissertation will now discuss an important conceptual understanding of mass surveillance provided by Jeremy Bentham and Michel Foucault.

The Panoptic Schema and Its Preventative Efficacity

The Panopticon (Greek for 'all seeing'), an exemplar institutional structure designed by English philosopher Jeremy Bentham in the late 1700's, was a circular building with a watchtower in the center. The outer building is divided into cells each having two windows, a wide window corresponding to the central watchtower, and a small one on the outer side to illuminate the cells. The watchtower's windows gaze upon the cells, but the watchtower's windows have blinds and the central tower is not illuminated, thus, allowing the guard to remain invisible. The architectural layout enables a single guard or supervisor in the central tower to see everyone in all the cells (Foucault, 1977, p.200). The backlighting allows the guard a clear view of the inmates, making them constantly visible and immediately recognizable, while keeping himself indiscernible.

For Bentham, the utility of the Panopticon was the economy and efficiency of monitoring everyone, as a single guard was needed to survey, collect data on the behaviors and activities of all inmates and analyze this information (Elmer, 2012). For Foucault, the disciplining ability was crucial, because the uncertainty and unverifiable nature of the guard's gaze, who may or may not even be present in the central tower, regulated the behaviors of the inmates. The Panopticon, thus, exercised power by inducing in the inmate a state of permanent visibility, because "in the peripheric ring, one is totally seen, without ever seeing; in the central tower, one sees everything without ever being seen" which regulated behavior (Foucault, 1977:201–202). This power was derived from an abundance of information (Tsui, 2003:69). Due to an asymmetry of knowledge in the Panopticon, caused by the doubtfulness of the gaze, there is a one-way flow of power (Kohl, 2013:187). According to Foucault, knowledge and power presuppose each other and are codependent, because knowledge without power is meaningless and in order to justify the exercise of power without resorting to force, knowledge is necessary (Foucault, 1977:27–28). For instance, this notion of "knowledge is power" was the underlying mentality of the US Information Awareness Office's total information awareness program for countering the risk of terrorism (Lyon and Haggerty, 2012).

Thus, it can be inferred that the Panopticon has two important functions for surveillance, 1) it allows the guard to monitor and collect knowledge constantly and act to mitigate risks; and 2) the permanent visibility of the inmate instills in him a particular discipline, to regulate his behavior and follow the norms of the prison. Of course, this does not mean that the inmates always conform to the rules and self-regulate themselves, resistance is also a feature as the inmates will either *feign* conformity as opposed to internalizing discipline or find alternative ways to evade the effects of power (Simon, 2005:8). However, even this resistance is ultimately corrected due to the effects of the power-knowledge nexus (this is further developed in Chapter 4 with respect to the Internet Panopticon).

In the past few decades, Foucault's conceptualization of the Panopticon has been used and abused as a model for analyzing surveillance in conjunction with the social, political and technological developments in contemporary society and international relations (Caluya, 2010). This Foucauldian mode of the Panopticon has also been critiqued by many commentators as having lost its creative potential for making sense of the complexity and totality of contemporary forms of surveillance (Haggerty, 2006). However, the value of Foucault's conceptualization of the

Panopticon lies not in making it into a generalizable model for explaining all forms of surveillance, but rather in understanding how certain technologies and the rationalities accompanying them, used for generating knowledge through visibility, resemble the Panopticon – essentially a tool for control and disciplining through knowledge. The Internet also has great value for surveillance and data-gathering. Therefore, it is important to compare the Internet and the Panopticon for their similar features and effects.

As the analysis in this chapter has shown, risk becomes a precautionary *dispositif* in the context of terrorism. This manifests in states' security agenda, leading to the legitimization of policies permitting mass surveillance. The precautionary technologies of surveillance then seek to pre-control risks by gathering knowledge. The Panopticon serves as an exemplary model for surveillance with its capabilities to constantly monitor, gather knowledge and internalize particular behaviors. With this in mind, the next section will analyze how the Internet serves as a Panopticon, which is then wielded by states as a precaution against terrorism.

CHAPTER THREE: The Internet Panopticon

The Panopticon theory has been applied to various forms of electronic surveillance assemblages, such as CCTV (Fussey, 2007) and biometric identification (Wilson, 2007), to explain the relevance and irrelevance of panopticism in contemporary society. The extent to which the Internet and social media networks are panoptic has also been analyzed. These studies have mainly focused on either the effects of workplace monitoring on employees' productivity or power relations between manufacturers/retailers with customers by collecting and analyzing data to discipline their behaviors towards commercial gains (Fuchs et al., 2011). Although an analysis of the Internet Panopticon similar to the one presented here was conducted by Lokman Tsui in the context of China; the ultimate dynamics of the Chinese case differ as they are driven by a complex authoritarian polity and carry the rationale of silencing dissent rather than preempting terrorism (Tsui, 2003).

In order to analyze the extent to which the Internet is a Panopticon, we ought to first look at some important and often overlooked aspects of the internet.

The Internet Never Forgets

Every time we use the internet, we constitute data representing some facts about ourselves on the cyberspace (Lessig, 2006:200). Internet technologies allow for cheap and constant monitoring of activities. These technologies make behavior more searchable, because online activities always leave records (ibid:203). Contrary to the popular understanding, attaining even a relative degree of anonymity on the internet is impossible since identifiable details about users such as Internet Protocol (IP) address and cookies (files containing device information, server name, user's preferences) are left behind with every activity. Curiosity is also monitored. For example, Google keeps a record of every search made, while also linking the IP address that made it to corresponding email accounts (Lessig, 2006:204). Emails get stored on various computers, browsers and servers that transmit them, unless removed either by humans or the machine itself. Emails can be monitored in real-time and retrospectively in order to know their content (Fuchs, 2011). Voicemail systems also record and archive messages on central servers of the service-provider. Voice recognition technology has advanced and this allows for searching through recorded messages for particular content (Lessig, 2006). Advertisers and marketers mine information that we put online, to paint quite detailed pictures of our lives, classify us into categories and track our behavioral patterns in order to have a predictive power (Andrejevic, 2012).

On the Internet, we are perpetually visible, we leave digital footprints which can be tracked and traced; unknown observers constantly, economically and efficiently monitor us and accumulate information; there is uncertainty as surveillance is not only automatic, but we don't know *who* exactly is observing *what* aspects of our online activities, and these observers crave for factual certainty via gathering knowledge (Lyon, 1994). In essence, these main

architectural features of the internet could be suggestive of its panoptic nature.

Panopticon or Not a Panopticon?

Despite the aforementioned features of the Internet, commentators have criticized the notion that modern surveillance technology, especially the Internet, is a Panopticon. These claims will be analyzed in the following sections.

1) Centralization

One of the main arguments for why the Internet does not amount to a Panopticon stems from the fact that, unlike the Panopticon where there are hierarchical power relations between the guards and the inmates, the Internet is decentralized (Boyle, 1997; Haggerty, 2006). In fact, the Internet is the antithesis of centralization because no single entity owns it and no single authority/individual can watch all Internet users (Mehta and Darier, 1998:108). Due to its decentralized nature, the Internet cannot be effectively regulated as there are several intermediaries, in the form of internet service providers (ISPs), internet companies and other technology corporations, to allow for total governmental control. Therefore, it is impossible to regulate information flows on the Internet (ibid).

However, this claim is unconvincing because, through its architectural structure, the Internet is actually a network of control. This is especially visible in authoritarian regimes, where public entities run the Internet under strict oversight conditions (Tsui, 2003). Moreover, even though the internet appears as *de*centralized, it is fundamentally a network of multiple centralized networks (Galloway, 2006:31). Governments 'tame' the Internet through the intermediaries that control these networks (Kohl, 2013). For instance, cyber laws are laid down to control various criminal activities, such as copyright infringements, pornography, cyber-hate through which states subtly but pervasively control the Internet (Clark, Brenson and Lin, 2014). Furthermore, when faced with security threats such as terrorism, governments wield stronger legislative apparatuses to make intermediaries comply (this will be explained in the next sections).

2) Enclosed Space

The original Panopticon allowed for constant observation, monitoring and functioning of power due to its architectural enclosure. Therefore, critics have argued that the Internet is not a Panopticon as it lacks a physically enclosing space which can guarantee control (Lippert, 2009; Haggerty and Ericson, 2000). They argue instead that the Internet allows users to transcend the boundaries of time and space due to the promulgation of a global network.

However, their argument is unconvincing as cyberspace in itself is enclosing. Cyberspace is built from code, the software and hardware that constitute the internet (Lessig, 2006). Cyberspace is controlled by this code, and as most users do not know how to alter this code, they are enclosed in the network. For instance, users cannot move freely over the internet. Based on where one is located geographically and jurisdictionally, access to certain areas on the net are restricted by ISPs or the government (Castells, 2001). Furthermore the increasing omnipresence of the Internet and ICTs can be experienced through the notion of "Internet of Things" whereby all our devices are integrated into one big network which gathers all the data it can about us to improve our experience (Burrus, 2014). This integration of devices and functions into everyday life creates a digital enclosure from which there is no place to hide (Andrejevic, 2007).

3) Unconcealed Surveillance

In the Panopticon, self-regulation and discipline was an attribute of overt visibility. The inmates were aware of their visibility, thus altering their behavior. Critics argue that the Internet is not a Panopticon because surveillance is covert, thus producing no disciplining effects, no "soul-training" (Haggerty, 2006; Foucault, 1977:201).

However, wider disciplining effects do emerge in the context of Internet surveillance even though the Internet was not designed to be explicitly disciplining with the aim of sheer social control (Lyon, 2003). People might believe they

are free in cyberspace as monitoring on the Internet is usually unobtrusive. However, critics fail to understand that most internet social networking platforms are audience based platforms, therefore, participants adhere to norms and often self-censor themselves (Tsui, 2003; Mehta and Darier, 1998). Likewise, there is always a suspicion that one is being watched or monitored on the internet as unlike in the real world, communications online always involve intermediaries or third-parties (in the form of ISPs/search engines/applications) (Peters, 1999; Kohl, 2013).

Following Edward Snowden's revelations in 2013, we now have good reason to suspect that our communications are being monitored. Research undertaken by institutions such as Pew and PEN International, have discovered these revelations have led to a global disciplining effect in the form of "global chilling" and a "spiral of silence" (Pen International, 2015; Hampton et al., 2014). Mass surveillance, even when undertaken with a view to mitigate just terrorism, induces a sense of self-censorship and moderates online behavior. Individuals conform to accepted socio-political norms, not voice opinions for fear of being misunderstood as dissent and refrain from engaging in behavior that would place one under the scrutiny of the government. Furthermore, people deliberately refrain from certain conversation topics or searches which are deemed controversial, such as terrorism for fear of inviting further surveillance (Pen International, 2015).

4) Human vs Machine

In the Panopticon, the guard in the central tower plays an important role for conducting surveillance and monitoring people. In the Internet Panopticon, surveillance is an automated function relying on computer softwares or algorithms that sift through communications. Hence, critics argue that the Internet is not a Panopticon because of the lack of human-to-human surveillance (Haggerty, 2006).

However, this criticism does not take into account the original functions of the Panopticon – to enable a continuous accumulation of knowledge about the inmates and an automatic functioning of power, regardless of who is in the watchtower, because they are ultimately invisible (Foucault, 1977). As has been already mentioned and will be more developed in the next section, governments conduct internet surveillance through more than one means and rely on private corporations to collect data and monitor people. Although, various automatic data capturing and analyzing devices are used, removing the need for human observers, ultimately the data is collected and available for government agents, intelligence agencies or private contractors to analyze and make judgements on. Furthermore, as stated in the previous section, Snowden's Revelations have led to a particular disciplining in populations even though it was revealed that surveillance is conducted by computer driven softwares and algorithms as opposed to human agents of the government. The effects of the gaze are the same, whether it is human or machine (Peters, 1999).

5) Docile Bodies

Critics further argue that the Internet cannot be equated to the Panopticon as the objects of internet surveillance are not docile but active participants (Haggerty, 2006; Poster, 1990). They claim that the inmates were disciplined and information gathered because inmates resigned themselves to the effects of permanent visibility in the Panopticon. There was no place to hide or escape. Contrary to this, Haggerty claims that individuals under internet surveillance are active as they have more scope for resisting Internet surveillance in their day-to-day routine (Haggerty, 2006:34). Moreover, he argues that internet users are active participants in their surveillance rather than being imprisoned in cyberspace (ibid).

While this dissertation does acknowledge the claim that Internet users actively use and constitute data about themselves on the cyber-sphere, however, they are not completely free from influence. As Foucault argues, governmental power works subtly (Foucault, 1991). It can either coerce or influence. The Internet Panopticon works by seducing users and normalizing them to participate online through the rewards the Internet has to offer, rather than punishments (Poster, 1990). For instance, users are now made to give up more personal details, such as mobile phone numbers during the registration process if they want to use Facebook to enjoy social connectivity.

As the above analysis has demonstrated, the Benthamite and Foucauldian concept of the Panopticon is relevant for

analyzing Internet surveillance. The Internet is a Panopticon without enclosing walls or central watch towers, where mostly machines are the guards. This is because the circuits of communication and the databases they create offer an unlimited surveillance capability (Poster, 1990:93). In this Panopticon, inmates are not completely docile, but actively participate in their surveillance, as they are normalized into accepting Internet technology and integrating it in their lives because of its rewards. The uncertainty of being watched, especially following Snowden's revelations, induces self-regulating discipline amongst users. The following section will now analyze 'how' this virtual Panopticon is enabled and used by states as a precautionary *dispositif* against the risk of terrorism.

Wielding the Internet Panopticon against the Risk of Terrorism

The Panopticon works through observation and classification (Lyon, 1998:94). As the above analysis has demonstrated, the Internet Panopticon offers an automatic form of surveillance and intelligence-gathering in the present, with access to data of the past to control future behavior (Elmer and Opel, 2006). This section will discuss the particular tactics of counter-terrorism used by governments to utilize Internet Panopticon, permitting constant monitoring and classifying populations into risk categories on the basis of their behavior. Although the Internet Panopticon is applicable to other countries, this paper will only analyze this in the US, the UK and Indian contexts, because they have faced major terrorist attacks, in the form of the 9/11 attack in New York, the London underground attacks in 2005 and the Mumbai terror attacks of 2006 and 2008; which have led to significant changes in their security policies (King's College London, 2015). These policies, which are discussed below, have enabled the governments to conduct mass surveillance programs, utilizing the Internet Panopticon to observe online behavior and classify populations into various categories allowing further control over their actions.

1) The US Panopticon

The Internet Panopticon in the US is enabled by two main legislations – the Uniting and Supporting America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 and the Foreign Intelligence Surveillance Act Amendments of 2008 (Kerr, 2002; GPO, 2015). These acts bestow vast powers on the US intelligence agencies, particularly the National Security Agency (NSA) to conduct internet and electronic surveillance as a measure to "sweep" terrorism (Greenwald, 2014). The measures undertaken by the NSA under this act include front-door access program PRISM, which collects communications content and metadata (data about data) about users directly from the servers of the world's largest Internet companies and UPSTREAM which conducts surveillance on real-time communications (Van Hoboken and Rubinstein, 2013). The US has a major advantage in exploiting the Internet Panopticon as most of the major Internet companies are operated under its jurisdiction, and 80% of the world's communications traffic has to traverse through the US (Lyon and Haggerty, 2012). PRISM allows the NSA to remotely and directly access communications from the networks of 9 global companies: Google, Microsoft, Facebook, Yahoo, Skype, Apple, Paltalk, YouTube and AOL (Bigo, Boulet, Bowden and Carrera, 2013; Greenwald, 2014:110). The program, then searches through large volumes of data looking for particular keywords and identifying patterns of correlation and connectivity, to separate them into different categories of risk (Inkster, 2013).

2) The UK Panopticon

In the UK, the Government Communications Headquarters (GCHQ) undertakes counterterrorism mass surveillance in conjunction with counter-terrorism bodies of the various government departments such as MI6. The main legislations enabling the Internet Panopticon, are the Data Retention and Investigatory Powers Act (DRIPA) 2014, the Regulation of Investigation and Powers Act (RIPA) 2000 and the Telecommunications Act 1984 (Home Office, 2014, Telecommunications Act 1984; Government of UK, 2015). Clause 94 of Telecommunications Act in particular lends the UK Secretary of State very broad authorities in national security or foreign relations interests, to compel the telecoms companies to undertake measures, such as installing interception devices (Telecommunications Act 1984, chap.VII; Greenwald, 2014). The biggest internet surveillance program under these laws is TEMPORA. It works by directly intercepting and extracting communications data from undersea fiber-optic cables, the backbone of the internet. It is reported that to accomplish this, the UK government has placed interceptors on around 200 cables around the British Isles, Europe and even the US (Bauman et al., 2014).

Furthermore, BULLRUN is a joint project between the NSA and GCHQ which intercepts data by defeating the encryption used online to safeguard details about transactions (Greenwald, 2014:94). It accomplishes this by relying on a range of stealthy methods such as supercomputers to break codes, pressuring software and internet companies to hand over their master encryption keys or build backdoors; and covertly introducing technical weaknesses into commercial encryption standards (Van Hoboken and Rubinstein, 2013:506).

3) Indian Panopticon

India started wielding the Internet Panoptic as a technology of taking precautions against the risk of terrorism following 2008. The Central Monitoring System (CMS) is a newly developed program, in line with the NSA and GCHQ, which commenced in 2013 (Xynou, 2015). CMS gets its authority from clause 41.10 of the Unified Access Services (UAS) License Agreement amendments of 2013, which allows it to place Interception Store and Forward (ISFs) systems on the networks of telecom providers to allow CMS direct and unrestricted access to communications (Department of Telecommunications and Ministry of Communications and IT, 2013). Prior to CMS, licensing agreements between the government and telecoms already required to have Lawful Interception Systems placed on the telecoms' servers (Singh, 2013). This does away with requiring warrants to access communication information from telecoms, as the CMS integrates, automates and centralizes the internet and other electronic surveillance activities of the Indian government (Xynou, 2014). The only oversight in place is the Indian Telegraph Act of 1885 which limits internet surveillance and data interception in the interests of public emergency/safety or for security reasons (Government of India, 2015, sec.5(2)). However, considering the risk of terrorism is defined broadly in the late-modern era and that everyone is a potential suspect, the oversights do not seem to hold up as it is difficult to distinguish between what is safety and what is not.

The analysis in this chapter has highlighted how the Internet is a virtual Panopticon due to its surveillance capabilities and the above section has highlighted the legislative tactics that allow governments to use this Panopticon against the risk of terrorism. There are significant implications of these above legislative policies and programs for counter-terrorism, as they enable governments to counter the difficulties associated with tracking and tracing terrorist networks, as they become increasingly diffused globally (Westby, 2006). The Internet Panopticon allows governments and intelligence agencies to monitor and analyze large sets of international communications and discern suspicious behavior patterns. They can, thus, pre-empt threats that may originate anywhere in the world and would be unknowable without this technology (Inkster, 2015). For instance, in 2010 GCHQ was able to identify an airline worker with links to Al-Qaeda and apprehended him before he could follow through on his plot (Inkster, 2015). Thus the Internet Panopticon, through its surveillance capabilities and the counter-terrorism legislation, is an important technology to the risk of terrorism because it functions as a precautionary *dispositif* to govern terrorism by gathering vast quantities of knowledge. However, recently, governments are facing increased scrutiny on the legitimacy of using this Internet Panopticon. The next chapter sheds a light on this.

CHAPTER FOUR: Confronting the Panopticon

Knowledge is power and the Internet Panopticon creates diffused power relationships between those who have access to its complex technological watch-tower and those utilizing internet enabled devices. However, as Foucault argues, "where there is power, there is resistance" (Foucault, 1978:195). With regards to Internet surveillance too, there are everyday forms of resistances such as simply not giving up information or providing false information, using proxy servers or privacy enhancing tools (PETs) to remain hidden or simply limiting ones presence in cyberspace to escape the gaze of the observers (Gilliom and Monahan, 2013:405). This resistance is usually diffused and distributed in an irregular fashion; quite similar to the network of relations through which power is exercised (ibid).

When these diffused points of resistance are strategically codified, there are counter-conducts. These counter-conducts can be seen as political struggles that aim to challenge the effects of state power. In the case of the Internet

Panopticon, the technological architecture, the legislative assemblages and the justifying rationalities provided by the risk of terrorism are challenged in real and cyber space. Although the broader objectives behind this resistance cannot be fully explored here, it should be noted that they are rather political, creating a tacit challenge and introducing symbolic friction to existing systems of control (Gilliom and Monahan, 2013:405).

In June 2013, Edward Snowden, a data analyst hired by the NSA, revealed the extent of the mass surveillance practices of the US and its western allies (Greenwald, 2014). Subsequently the past few years revealed similar mass surveillance programs in other countries, such as India and Pakistan (Singh, 2013; Lakshman, 2015). Surveillance has now become a civil problem in not just western democracies. Moreover, the revelations exposed that mass surveillance was conducted for mining personal information of large populations to analyze political opinions, industrial espionage and spying on politicians superimposed against the wider rhetoric of a shared struggle against the risk of terrorism (Bauman et al., 2014:127). This has led to a resistance movement opposing the whole discourse of security and surveillance which enables the Internet Panopticon as a precautionary *dispositif* of the risk of terrorism.

The prime resistance to this Panopticon has emerged from the Brazilian and German governments. Following Snowden's Revelations, Brazilian President Rousseff raised and pursued the issues of gross human rights violation and disrespect to national sovereignty in the United Nations General Assembly (UNGA), condemning NSA and GCHQ (Bauman et al., 2014:128). This resulted in a noticeable push for including privacy rights on the UN Human Rights Committee's agenda and led to the adoption of the UNGA Resolution for Privacy Rights in a Digital Age (Grigsby, 2014).

Moreover, NGOs such as Privacy International and Amnesty have begun staunchly advocating against unlawful mass surveillance and pushing for discontinuing bulk-data collection by citing a violation of the rights to privacy and freedom of speech and expression (Fulton, 2015). Success stories of these advocacy movements can be seen in the number of cases brought against governments in international courts, demanding reform of the legislation authorizing Internet surveillance (Amnesty International, 2015a). For instance, the USA FREEDOM Act of May 2015 is a new legislation putting drastic limits to the bulk collection capabilities of the US government (Amnesty International, 2015b:4).

There is a strong push worldwide, from privacy activists, concerned citizens and also national-governments, to curb the overreaching activities of intelligence agencies such as the NSA and GCHQ. There are discussions about localization of the internet, wherein ISPs and Internet companies would be required to locate their operations inside the country where the services are offered, making citizens data locally-stored, and restricting unlawful data interception by the major foreign intelligence agencies (Llanso, 2014; Van Hoboken and Rubinstein, 2013). In particular, Brazil and EU countries are discussing massive infrastructural changes to keep traffic local and isolate their systems from falling prey to foreign surveillance. Brazil is planning to expand its international Internet connectivity by constructing its own undersea and overland fiber-optic cables, and integrating South American and BRICS countries in its own network to counter the US influence in cyberspace (Bauman et al., 2014). However, resisting the huge Internet Panopticon created by superpowers like the US and its allies, will not lead to an isolated, localized Internet free from panoptic surveillance. Localization would simply provide national governments with total access to Internet communications based on national laws, control over the fiber-optic infrastructure and regardless, the authority to insist on easy access to servers under the rubric of security interests (Llanso, 2014).

Furthermore, ISPs, telecoms, tech companies like Google, Apple, Yahoo and various other Internet platforms are also resisting state power due to the public scrutiny they faced on grounds of cooperating and providing intelligence agencies easier access to data (Levy, 2014). Internet companies require the trust and willingness of their customers to use their technology and provide information. However, this trust was undermined by the revelations of mass surveillance. These companies have now been caught up in the web of strengthening encryption to make their systems more secure and being compelled to provide information. Companies like Facebook, Apple and Google now provide default end-to-end encryption on their services, where only endpoint computers can decrypt the message ensuring the companies themselves are not privy to these communications (Miller, 2014; Greenberg, 2014). This allows companies to restrict direct access to government agencies as they themselves do not have access to the

exact communication information. Moreover, many tech companies are also strengthening their regular encryption systems (such as Secure Socket Layer, the most commonly used encryption) and not building any "back-doors" to restrict access to governments agencies and treating them are "third-party agents" (Van Hoboken and Rubinstein, 2013).

However, this resistance in the form of encryption, both on the side of the companies and the rapidly increasing trend of internet users themselves encrypting their messages using softwares such as PGP (Pretty Good Privacy), is viewed as a risk to national security (Lewis, 2014). In the late modern-era, faced with numerous uncertainties and unknown risks, governments need to know everything, in order to take precautions. However, encrypting communications in a way that restricts government access turns encryption into a risk, an obstacle that must be destroyed. This is highlighted by the statements of top government officials, such as Prime Minister David Cameron who exclaimed that he was not going to allows a means of communication which was impossible to read (Cameron Quoted in Zittrain, 2015). A wider rhetoric of encrypted messaging and online services as enabling "dark spaces" for terrorists to recruit, radicalize, plot and plan is being circulated as a political rationale, calling for legal remedies to allow access to encrypted communications (Price, 2015b). This might also lead to countries like the UK and USA following the example of Russia, China and other rigid polities to put total ban or increased restrictions on the use of encryption (see also David Cameron's quest for banning encryption in the UK in Price, 2015a).

Furthermore, internet users using encryption, PETs or simply because of searching for such tools are automatically targeted for tracking and monitoring (Zetter, 2014). Softwares like XKeyscore, used by the NSA, allow identifying and tagging online activity, in order to sort data on the basis of users' online activities (ibid). This allows the NSA to track particular IP addresses who visit websites of privacy enhancing browsers including Tor, FreeProxies.org and FreeNet.

Resistance to power is inevitable, but, the Internet Panopticon and the overarching specter of risks make it unlikely for this resistance to be effective. This is due to the main difference of resources and skills – between the powerful states like the US who access the Internet Panopticon and other smaller countries like Brazil and also between states and civil society actors. Compared to other adversaries, intelligence and defense agencies have unfettered access to finance, world-class technology and expertise (Van Hoboken and Rubinstein, 2013:493). Furthermore, intelligence is usually gathered by cooperating with allied agencies with similar or better capabilities. This acts like a force multiplier as is evident in the case of the "Five Eyes" partners – the US, the UK, Australia, Canada and New Zealand (ibid). This is similar to Foucault's description of the nature of resistance and its relation to power, "where there is power, there is resistance", but ultimately, "this resistance is never in a position of exteriority in relation to power" (Foucault, 1978, p.95). Thus, resistance to the Internet Panopticon will not oppose its power, but co-produces it, while making visible its controlling nature (Gilliom and Monahan, 2013).

CHAPTER FIVE: Conclusion

Technological developments are a double-edged sword, they bring with them countless benefits like effortless communication and convenience, but they also produce malicious and unknown risks which can cause irremediable damages. As this paper has attempted to demonstrate, to govern the risk of terrorism, governments embark on an insatiable quest for knowledge. With the advent of the Internet and cyberspace, the risk of terrorism is augmented, because cyberspace provides terrorism not only with a new medium to spread its global network, but also with the possibility to use the cyberspace as a weapon of mass disruption. However, this cyberspace, which has a potential for generating knowledge, in turn is used by governments to control and take precautions against the risk of terrorism.

With over 3 billion users (and the numbers are constantly on the rise), the Internet has vast potential for surveillance activities because it has become so ubiquitous and integrated with our lives. As this paper has shown, the Internet is

a Panopticon because our activities are monitored, recorded and tracked; we do not know if or when we are under surveillance or even who is conducting it. Moreover, the Internet Panopticon normalizes and disciplines our behavior, making us participate in our own surveillance. Following Snowden's revelations, the Internet Panopticon has exhibited its potential to further discipline our behavior, to silence dissent and turn us into docile bodies subordinated to the government's power.

As demonstrated in Chapter 3, the cases of the online mass surveillance legislations and apparatuses in the US, the UK and India constitute practical evidence of the usefulness of the Panopticon as a useful metaphor for analyzing Internet Surveillance in an age of terror.

BIBLIOGRAPHY

Amnesty International. "Two Years After Snowden Governments Resist Calls to End Mass Surveillance."*Amnesty International*, June 5, 2015. https://www.amnesty.org/en/press-releases/2015/06/two-years-after-snowden/.

———. "Two Years After Snowden: Protecting Human Rights in an Age of Mass Surveillance." London: Amnesty International, June 4, 2015. https://www.amnesty.org/en/documents/act30/1795/2015/en/.

Amoore, Louise, and Marieke de Goede, eds. *Risk and the War on Terror*. London ; New York: Routledge, 2008.

Andrejevic, Mark. "Exploitation in the Data Mine." In *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, edited by Christian Fuchs, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval, 71–88. New York: Routledge, 2012.

———. "Surveillance in the Digital Enclosure." *The Communication Review* 10, no. 4 (December 5, 2007): 295–317. doi:10.1080/10714420701715365.

Aradau, Claudia, Luis Lobo-Guerrero, and Rens Van Munster. "Security, Technologies of Risk, and the Political: Guest Editors' Introduction." *Security Dialogue* 39, no. 2–3 (April 1, 2008): 147–54. doi:10.1177/0967010608089159.

Aradau, Claudia, and Rens Van Munster. "Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future." *European Journal of International Relations* 13, no. 1 (March 1, 2007): 89–115. doi:10.1177/1354066107074290.

Awan, Imran, and Brian Blakemore. *Policing Cyber Hate, Cyber Threats and Cyber Terrorism*. New edition edition. Farnham ; Burlington, VT: Ashgate, 2012.

Baker, Stewart. "Remarks." Washington: Center for Strategic and International Studies, 2006. http://webcache.googleusercontent.com/search?q=cache:QXmJMWAG-24J:https://www.hsdl.org/%3Fview%26did%3D474379+&cd=2&hl=en&ct=clnk&gl=uk.

Barnard-Wills, David, and Debi Ashenden. "Securing Virtual Space Cyber War, Cyber Terror, and Risk."*Space and Culture* 15, no. 2 (May 1, 2012): 110–23. doi:10.1177/1206331211430016.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B. J. Walker. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8, no. 2 (June 1, 2014): 121–44. doi:10.1111/ips.12048.

Beck, Ulrich. “The Terrorist Threat World Risk Society Revisited.” *Theory, Culture & Society* 19, no. 4 (August 1, 2002): 39–55. doi:10.1177/0263276402019004003.

Beck, Ulrich, and Scott Lash. *Risk Society: Towards a New Modernity*. Translated by Mark Ritter. London ; Newbury Park, Calif: Sage Publications UK, 1992.

Bigo, Didier, Gertjan Boulet, Caspar Bowden, and Sergio Carrera. “Open Season for Data Fishing on the Web: The Challenges of the US PRISM Programme for the EU. CEPS Policy Brief No. 293, 18 June 2013.” Policy Paper, 2013. http://ceps.eu/book/open-season-data-fishing-web-challenges-us-prism-programme-eu.

Boyle, James. “Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors.”*University of Cincinnati Law Review* 66 (January 1, 1997): 177–205.

Burchell, Graham, Colin Gordon, and Peter Miller, eds. *The Foucault Effect: Studies in Governmentality*. Chicago: University of Chicago Press, 1991.

Burrus, Daniel. “The Internet of Things Is Far Bigger Than Anyone Realizes.” *WIRED*, November 21, 2014. http://www.wired.com/insights/2014/11/the-internet-of-things-bigger/.

Caluya, Gilbert. “The Post-Panoptic Society? Reassessing Foucault in Surveillance Studies.” *Social Identities* 16, no. 5 (September 1, 2010): 621–33.

Castells, Manuel. *The Internet Galaxy: Reflections on the Internet, Business, and Society* . Oxford ; New York: OUP Oxford, 2001.

Ceyhan, Ayse. “Surveillance as Biopower.” In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin D. Haggerty, and David Lyon, 38–45. New York: Routledge, 2012.

Clapton, William. “Risk and Hierarchy in International Society.” *Global Change, Peace & Security* 21, no. 1 (February 1, 2009): 19–35. doi:10.1080/14781150802659267.

———. “Risk in International Relations.” *International Relations* 25, no. 3 (September 1, 2011): 280–95. doi:10.1177/0047117811415480.

Clark, David, Thomas Brenson, and Herbert S. Lin, eds. *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. Washington: The National Academies Press, 2014. http://www.nap.edu/openbook.php?record_id=18749.

Clarke, Roger. “Information Technology and Dataveillance.” *Communications of the ACM* 31, no. 5 (May 1988): 498–512.

Department of Telecommunications, and Ministry of Communications and IT. “Amendment to the UAS License Agreement Regarding Central Monitoring System.” Government of India, 2013. cis-india.org/internet-governance/blog/uas-license-agreement-amendment.

Diez, Thomas, Ingvild Bode, and Aleksandra Fernandes da da Costa. *Key Concepts in International Relations*. Los Angeles ; London: SAGE Publications Ltd, 2011.

Doty, Philip. “U.S. Homeland Security and Risk Assessment.” *Government Information Quarterly* 32, no. 3 (July 2015): 342–52. doi:10.1016/j.giq.2015.04.008.

Elmer, Greg, and Andy Opel. “Pre-Empting Panoptic Surveillance: Surviving the Inevitable War on Terror.” In *Theorizing Surveilance: The Panopticon and beyond*, edited by David Lyon, 139–60. Cullompton, Devon: Willan,

2006.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. Translated by Alan Sheridan. London: Penguin, 1977.

———. “Governmentality.” In *The Foucault Effect: Studies in Governmentality*, edited by Graham Burchell, Colin Gordon, and Peter Miller, 87–104. Chicago, 1991.

———. *The History of Sexuality: An Introduction*. Translated by Robert Hurley. Vol. 1. New York: Random House, 1978.

Fuchs, Christian. “New Media, Web 2.0 and Surveillance.” *Sociology Compass* 5, no. 2 (2011): 134–47.

Fuchs, Christian, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval, eds. *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. New York: Routledge, 2011.

Fulton, Sandra. “Unlikely Allies Unite Against Mass Surveillance.” *Free Press*, March 25, 2015. http://www.freepress.net/blog/2015/03/25/unlikely-allies-unite-against-mass-surveillance.

Furedi, Frank. *Culture of Fear: Risk-Taking and the Morality of Low Expectation Revised Edition*. A&C Black, 2002.

Fussey, Pete. “Observing Potentiality in the Global City: Surveillance and Counterterrorism in London.” *International Criminal Justice Review* 17, no. 3 (2007): 171–92.

Galloway, Alexander R. *Protocol: How Control Exists After Decentralization*. New Ed edition. Cambridge, Mass.: MIT Press, 2006.

Gilliom, John, and Torin Monahan. “Everyday Resistance.” In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin D. Haggerty, and David Lyon, 405–11. New York: Routledge, 2013.

Google. “Major Al-Qaeda Attacks Worldwide,” August 25, 2015. https://www.google.com/maps/d/viewer?mid=ze5Idz9dcH7o.kglDu_OmVKUA&hl=en_US.

Government of India. “Indian Telegraph Act.” Offical Government Website. *Department of Telecommunications*, 2015. http://www.dot.gov.in/act-and-rules/indian-telegraph-act.

Government of UK. “A Strong Britain in an Age of Uncertainty: The National Security Strategy,” 2010. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

———. “Regulation of Investigatory Powers Act 2000.” *UK Legislation*, 2015. http://www.legislation.gov.uk/ukpga/2000/23/contents.

GPO. “Text of H.R. 6304 (110th): FISA Amendments Act of 2008 (Passed Congress/Enrolled Bill Version).” *US Government Publishing Office*. Accessed August 31, 2015. http://www.gpo.gov/fdsys/search/pagedetails.action?packageId=BILLS-110hr6304enr.

Greathouse, Craig B. “Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?” In *Cyberspace and International Relations*, edited by Jan-Frederik Kremer and Benedikt Müller, 21–40. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

Greenberg, Andy. “Hacker Lexicon: What Is End-to-End Encryption?” *WIRED*, November 25, 2014. http://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.

Greenwald, Glenn. *No Place to Hide*. London: Penguin, 2014.

Grigsby, Alex. "UN Committee Adopts Resolution on Right to Privacy in the Digital Age." *Council on Foreign Relations – Net Politics*, December 1, 2014. http://blogs.cfr.org/cyber/2014/12/01/un-committee-adopts-resolution-on-right-to-privacy-in-the-digital-age/.

Guldberg, Helene. "Challenging the Precautionary Principle." *Sp!ked*, July 1, 2003. http://www.spiked-online.com/newsite/article/challenging_the_precautionary_principle/5085.

Hacking, Ian. *The Taming of Chance*. Cambridge England ; New York: Cambridge University Press, 1990.

Haggerty, Kevin D. "Tear down the Walls: On Demolishing the Panopticon." In *Theorizing Surveilance: The Panopticon and beyond*, edited by David Lyon, 23–45. Cullompton, Devon: Willan, 2006.

Haggerty, Kevin D., and Richard V. Ericson. "The Surveillant Assemblage." *The British Journal of Sociology* 51, no. 4 (December 1, 2000): 605–22.

Hampton, Keith, Lee Rainie, Weixu Lu, Maria Dwyer, Inyoung Shin, and Kristen Purcell. "Social Media and the 'Spiral of Silence.'" Pew Research Center, August 26, 2014. http://www.pewinternet.org/2014/08/26/social-media-and-the-spiral-of-silence/.

Heng, Yee-Kuang. "The 'Transformation of War' Debate: Through the Looking Glass of Ulrich Beck's World Risk Society." *International Relations* 20, no. 1 (March 1, 2006): 69–91. doi:10.1177/0047117806060929.

Home Office. "Data Retention and Investigatory Powers Act 2014 – GOV.UK." Government. *Government of UK*, July 25, 2014. https://www.gov.uk/government/collections/data-retention-and-investigatory-powers-act-2014.

Inkster, Nigel. "Communications Interception: UK Report Seeks Legal Reform." *Strategic Comments* 21, no. 18 (2015).

———. "Surveillance and Counter-Terrorism." *Politics and Strategy: The Survival Editors' Blog*, October 14, 2013.

internetlivestats.com. "Internet Live Stats." *Internetstatslive.com*, August 12, 2015. http://www.internetlivestats.com/.

Jensen, Carl J., David H. McElreath, and Melissa Graves. *Introduction to Intelligence Studies*. Boca Raton: CRC Press, 2013.

Kerr, Orin S. "Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, July 19, 2002. http://papers.ssrn.com/abstract=317501.

King's College London. "How Did These Terror Attacks during the Last 20 Years Change the World?," July 23, 2015, sec. World. http://www.telegraph.co.uk/news/worldnews/islamic-state/11729063/How-did-these-terror-attacks-during-the-last-20-years-change-the-world.html.

Knake, Robert K. *Internet Governance in an Age of Cyber Insecurity*. New York, NY: Council on Foreign Relations, 2010.

Kohl, Uta. "Google: The Rise and Rise of Online Intermediaries in the Governance of the Internet and beyond (Part 2)." *International Journal of Law and Information Technology* 21, no. 2 (June 1, 2013): 187–234.

Lakshman, Narayan. "Pakistan Has Built a Massive Surveillance State: Report." *The Hindu*. July 25, 2015. http://www.thehindu.com/news/international/south-asia/pakistan-has-built-a-massive-surveillance-state-report/article7462002.ece.

Lemke, Thomas. “Foucault, Governmentality, and Critique.” *Rethinking Marxism* 14, no. 3 (September 1, 2002): 49–64.

Lessig, Lawrence. *Code: And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books, 2006.

Levy, Steven. “How the NSA Almost Killed the Internet.” *WIRED*, January 7, 2014. http://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/.

Lewis, James A. “2104 as the Year of Encryption: A (Very) Brief History of Encryption Policy.” *CSIS*, January 10, 2014.

Lippert, Randy. “Signs of the Surveillant Assemblage: Privacy Regulation, Urban CCTV, and Governmentality.” *Social & Legal Studies* 18, no. 4 (December 1, 2009): 505–22. doi:10.1177/0964663909345096.

Llanso, Emma. “How Politicians Are Trying to Break the Internet.” *CNN*, September 5, 2014. http://www.cnn.com/2014/09/05/business/opinion-internet-post-snowden/index.html.

Lyon, David. *Electronic Eye: The Rise of Surveillance Society*. 1 edition. Minneapolis: Univ Of Minnesota Press, 1994.

———. “Technology vs ‘Terrorism’: Circuits of City Surveillance since September 11th.” *International Journal of Urban and Regional Research* 27, no. 3 (September 2003): 666–78.

———. *The Electronic Eye: The Rise of Surveillance Society – Computers and Social Control in Context* . John Wiley & Sons, 2013.

———. , ed. *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton, Devon: Willan, 2006.

———. “The World Wide Web of Surveillance: The Internet and Off-world Power-flows.” *Information, Communication & Society* 1, no. 1 (March 1, 1998): 91–105. doi:10.1080/13691189809358955.

Lyon, David, and Kevin D. Haggerty. “Surveillance Legacies of 9/11: Recalling, Reflecting On, and Rethinking Surveillance in the Security Era, The.” *Canadian Journal of Law & Society* 27, no. 3 (2012): 291.

Mehta, Michael D., and Eric Darier. “Virtual Control and Discipling on the Internet: Electronic Governmentality in the New Wired World.” *The Information Society* 14 (1998): 107–16.

Miller, Joe Miller Technology. “Google and Apple to Introduce Default Encryption.” *BBC News*, September 19, 2014. http://www.bbc.co.uk/news/technology-29276955.

Mythen, Gabe, and Sandra Walklate. “Criminology and Terrorism Which Thesis? Risk Society or Governmentality?” *British Journal of Criminology* 46, no. 3 (May 1, 2006): 379–98. doi:10.1093/bjc/azi074.

———. “Terrorism, Risk and International Security: The Perils of Asking ‘What If?’” *Security Dialogue* 39, no. 2–3 (April 1, 2008): 221–42. doi:10.1177/0967010608088776.

NATO Review. “The History of Cyber Attacks – a Timeline.” *NATO Review*. Accessed August 24, 2015. http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm.

O’Malley, Pat. “Governmentality and Risk.” SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, September 1, 2009. http://papers.ssrn.com/abstract=1478289.

Pen International. “Global Chilling: The Impact of Mass Surveillance on International Writers.” PEN American Center,

2015. http://www.pen-international.org/wp-content/uploads/2015/01/Global-Chilling_01-05-15_FINAL.pdf.

Peters, Thomas A. *Computerized Monitoring and Online Privacy*. McFarland, 1999.

Poster, Mark. *The Mode of Information: Poststructuralism and Social Context*. 2nd edition. Chicago: University of Chicago Press, 1990.

Price, Rob. "David Cameron Wants To Ban Encryption." *Business Insider*, January 12, 2015. http://uk.businessinsider.com/david-cameron-encryption-apple-pgp-2015-1.

———. "The FBI Claims Technology Promoted by Apple and WhatsApp Is Helping ISIS." *Business Insider*, June 4, 2015. http://uk.businessinsider.com/fbi-encryption-going-dark-isis-apple-facebook-whatsapp-steinbach-lieu-2015-6.

Radu, Roxana. "Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace." In *Cyberspace and International Relations*, edited by Jan-Frederik Kremer and Benedikt Müller, 3–20. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

Rasmussen, Mikkel Vedby. "`It Sounds Like a Riddle': Security Studies, the War on Terror and Risk."*Millennium – Journal of International Studies* 33, no. 2 (March 1, 2004): 381–95. doi:10.1177/03058298040330020601.

Renard, Thomas. "The Rise of Cyber-Diplomacy: The EU, It's Strategic Partners and Cyber-Security." ESPO working paper. Eurostrategic Partnerships and Transnational Threats. European Strategic Partnerships Observatory, 2014. http://strategicpartnerships.eu/2014/06/the-rise-of-cyber-diplomacy/.

Rotenberg, Marc, Jeramie Scott, and Julia Horwitz. *Privacy in the Modern Age: The Search for Solutions*. New Press, The, 2015.

Russett, Preston C. "A Contemporary Portrait of Information Privacy: Collective Commuicative Consequences of Being Digital." *The Review of Communication* 11, no. 1 (2011): 39–50.

Simon, Bart. "The Return of Panopticism: Supervision, Subjection and the New Surveillance." *Surveillance & Society* 3, no. 1 (2005): 1–20.

Singh, Shalini. "Govt. Violates Privacy Safeguards to Secretly Monitor Internet Traffic." *The Hindu*. September 8, 2013. http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece.

The White House. "National Security Strategy." The White House, February 2015. https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

Tsui, Lokman. "The Panopticon as the Antithesis of a Space of Freedom Control and Regulation of the Internet in China." *China Information* 17, no. 2 (October 1, 2003): 65–82.

UK Legislation. *Telecommunications Act 1984*, 1984. http://www.legislation.gov.uk/ukpga/1984/12/section/94.

van Heuven, Marten, Maarten Botterman, and Stephan De Spiegeleire. "Managing New Issues: Cyber Security in an Era of Technological Change." Product Page. Santa Monica, 2003. http://www.rand.org/pubs/monograph_reports/MR1535.html.

Van Hoboken, Joris V. J., and Ira S. Rubinstein. "Privacy and Security in the Cloud: Some Realism about Technical Solutions to Transnational Surveillance in the Post-Snowden Era." *Maine Law Review* 66 (2014 2013): 487–533.

Weinstein, C., W. Campbell, Brian Delaney, and G. O'Leary. "Modeling and Detection Techniques for Counter-Terror

Social Network Analysis and Intent Recognition." In *2009 IEEE Aerospace Conference*, 1–16, 2009.

Westby, Jody R. "Countering Terrorism with Cyber Security." *Jurimetrics* 47 (2007 2006): 297–313.

Williams, M. J. "(In)Security Studies, Reflexive Modernization and the Risk Society." *Cooperation and Conflict* 43, no. 1 (March 1, 2008): 57–79. doi:10.1177/0010836707086737.

Williams, Nik. "The Cost of Silence: Mass Surveillance & Self-Censorship." *openDemocracy*, April 6, 2015. https://www.opendemocracy.net/nik-williams/cost-of-silence-mass-surveillance-selfcensorship.

Wilson, Dean. "Australian Biometrics and Global Surveillance." *International Criminal Justice Review* 17, no. 3 (2007): 207–19.

Wyld, David C., Michal Wozniak, Nabendu Chaki, Natarajan Meghanathan, and Dhinaharan Nagamalai.*Trends in Network and Communications: International Conferences, NeCOM 2011, WeST 2011, and WiMON 2011, Chennai, India, July 15-17, 2011, Proceedings*. Springer Science & Business Media, 2011.

Xynou, Maria. "Big Democracy, Big Surveillance: India's Surveillance State." *openDemocracy*, February 14, 2014. https://www.opendemocracy.net/opensecurity/maria-xynou/big-democracy-big-surveillance-indias-surveillance-state.

———. "India's Central Monitoring System (CMS): Something to Worry About?" *The Centre for Internet and Society*. Accessed September 10, 2015. http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about.

Zetter, Kim. "Use Privacy Services? The NSA Is Probably Tracking You (Wired UK)." *Wired UK*, July 4, 2014. http://www.wired.co.uk/news/archive/2014-07/04/nsa-targeting-tor-users.

Zittrain, Jonathan. "Tyrants Will Find the Key to the Internet's Back Door." *Financial Times*, February 2, 2015. http://www.ft.com/cms/s/0/e99017f2-a572-11e4-ad35-00144feab7de.html#axzz3iRLcIEft.

Written by: Rudhayaini Vijay Mukane
Written at: The School of Oriental and African Studies, University of London
Written for: Ms Sruthi Muraleedharan
Date written: 12/2015