Traffic Analysis, Anonymity, Freedom and digital “Cat and Mouse” in Cyberspace: A case study of China vs Iran

Cameron J. Shahab
King’s College London
University of London
London, United Kingdom

Reza Mousoli
Computing Department
Canterbury Christ Church University
Canterbury, Kent, United Kingdom

Abstract
This paper aims to compare Chinese and Iranian cyberspace to highlight the excessive traffic analysis, surveillance, filtering and the resulting effects on anonymity and freedom of expression in the borderless society of the Internet. The paradoxical contrasts between these two different states provide much scope for analysis and discourse, particularly in light of recent media attention. As has been shown by the government crackdowns in the aftermath of the Iranian election of 2009, and China’s recent dispute with Google, cyberspace is highly contested by government’s seeking to harness digital economic and e-business benefits whilst restricting online dissent and political activism. Interdisciplinary by its very nature, this paper will investigate the ongoing ‘cat and mouse’ game between the authoritarian governments and how tools such as TOR, Mixminion, Incognito and Anonymizer are helping dissenters to hide their identity and stay anonymous. The multifaceted approach to the research consisted of semi-structured interviews with key actors, interviews with Iranian and Chinese citizens currently in the UK, focus groups and textual analysis of websites and blogs. This paper has shown the increase in traffic analysis and surveillance in both Iran and China. On the other hand, in this digital “cat and mouse” game, protesters persistently get their message out and access forbidden and filtered sites. The various tools used to bypass filters and restrictions have been outlined and briefly assessed, and the role of the new digital media landscape in shaping the political debates has been discussed. The Chinese government has been very successful in creating a society in which the state not only controls cyberspace for high e-commerce growth, but also uses it as a tool for reinforcing social control. From the interviews with Chinese citizens it was clear that although they were aware of the traffic analysis and filtering and surveillance, most were unconcerned, even considering it normal. In contrast, the Iranian citizens interviewed were extremely unhappy with the increasing trend towards surveillance, filtering and the limit on connection speed within Iran. The Iranian government has not been able to subtly enforce its control over cyberspace.
Unlike China where there are large e-transaction activities and huge online commercial interests, Iran still rely heavily on traditional commerce (Bazaar) and lacks advanced IT infra structure, expertise and software tools for traffic analysis and filtering; instead they have relied on slowing the entire Internet or bringing the system to a halt completely to deter protesters.

**Keywords**: privacy, traffic analysis, anonymity, freedom, cyberspace, China, Iran, tor, mixminion, incognito, anonymizer, anonymous, surveillance, filtering, ethics, “Open Net Initiative”, ONI, bbc Persian, voa, gooyanews, jingjing, chacha, panopticon, censorship, e-business, golden shield, Reporters Sans Frontiers, rsf.

1. Introduction

Cyberspace, a term coined by the author William Gibson (1980) in his novel Neuromancer has now become a universal term to describe anything and everything related to computers, information technologies and the Internet. Although Batty (1997) provides quite a clear definition of what cyberspace is, “interactivity between remote computers” (Batty, 1997: 343), it is used in this paper more generally to describe the Internet and digital media technologies. Iran and China both employ some of the most aggressive cyberspace censorship and surveillance programs (ONI, 2009a). In Iran, sites that are blocked are deemed “Immoral”, in China, “Subversive” (Tait, 2006b). Both States control and monitor their networks, and employ extensive, multifaceted surveillance aimed at controlling information and preventing dissent. Both Iran and China have recently been challenged by the new possibilities created by the growth of the Internet and digital media in recent years, and have adopted similar responses in order to deal with the threats to control. Iran and China have experienced rapid growth in the uptake of the Internet; China now has the highest number of Internet users in the world, around 300 million according to recent estimates (ONI, 2009a) and Iran has the most Internet users in the Middle East, approaching 30 million according to recent estimates (ONI, 2009b). Iran has one of the most vibrant and diverse Blogging communities; Farsi (Persian) is reportedly the fourth most popular Blogging language on the Internet (Rigby, 2006). Over the course of the last decade, Blogs have become one of the primary outlets for Iranians to express themselves with less fear of repression or political repercussions. This last refuge for free speech and free thought in Iran has now been compromised by the government’s increased restrictions and surveillance. Consequently, Iranian and Chinese dissipents are becoming more intelligent and sophisticated in using open source software tools to bypass filters and monitoring stations and are able to transmit and receive information online despite restrictions.
2. Censorship and Surveillance

Michel Foucault’s (1977) reinterpretation of Bentham’s (1785) Panopticon in ‘Discipline and Punish’ provides the theoretical grounding for many theorists when approaching the issue of surveillance. Using Bentham’s idealised prison as a metaphor Foucault considers the methods employed by society to encourage discipline and normalising behaviours.

“Whenver one is dealing with a multiplicity of individuals on whom a task or a particular form of behaviour must be imposed, the panoptic schema may be used” (Foucault, 1977:205)

Although Foucault never wrote directly on the panoptic power of the Internet, many authors have taken his work and adapted his theories to shed light on emergent technologies (Tsui, 2003). Cyberspace has become a central discourse in recent thinking about the panopticon and its effects on society. The concept of the panopticon prison is reliant upon the uncertainty of being monitored, in effect normalizing behaviour causing the individual to exhibit ‘anticipatory conformity’.

The Internet allows the state greater scope for surveillance, using computers to analyse data that in the past would have required a Stasi like organization and resources.

In Foucault’s (1978) own writings on Iran he was highly critical of Mohammed Shah Reza Pahlavi’s capitalist dictatorship and he wrote in praise of Islam, describing it as “a religion that gave to its people infinite resources to resist state power”. Foucault was particularly critical of the surveillance methods and disciplinary practices of the Shah and secret police, “The man with the iron hand is Moghadam, the leader of the SAVAK” (Foucault, 1978).

Many critics have considered these writings to be flawed – a “miscalculation” or “not Foucauldian” (Afray and Anderson, 2005). Foucault’s prescience foresaw the importance of the Islamic Revolution in Iran, that it could “set the entire region afire” (Foucault, 1978), but failed to anticipate the Islamic government’s own misuse of power, instead optimistically hoping for a ‘spiritually enlightened’ government for the people.

Censorship and surveillance are two tools used to control, normalise and limit behaviour (Foucault, 1977). Censorship involves blocking access to information or restricting free speech. Surveillance involves monitoring individuals or organisations. In Iran, censored websites are deemed ‘Immoral’ and “unethical”, in China, ‘Subversive’. When Internet users in these countries attempt to access sites that have been restricted by the state, they are often confronted by a warning message. Furthermore, in China, Internet users are repeatedly confronted by images of ‘Jingjing’ and ‘Chacha’, the Internet police (see Image 1, Source: Wikipedia)

---

1 SAVAK –The secret police under the Shah
Ostertag (2009) highlights the important differences between censorship and surveillance, particularly in Iran. Whilst censorship is simply a matter of intercepting and blocking communications (a difficult task), surveillance and traffic analysis on the Internet allows the information trail to be reconstructed, often providing identities and locations of the source/destination of data packets. In Iran, there are many rumours of dissenters being tracked by their electronic trail, enabling the authorities to arrest or abduct people, which given Iran’s human rights record is very worrying.

Google (2010) recently expressed grave concerns over censorship and surveillance in China after a hacking attack on gmail accounts, particularly those involved in Human Rights in China:

“These attacks and the surveillance they have uncovered—combined with the attempts over the past year to further limit free speech on the web—have led us to conclude that we should review the feasibility of our business operations in China. We have decided we are no longer willing to continue censoring our results on Google.cn, and so over the next few weeks we will be discussing with the Chinese government the basis on which we could operate an unfiltered search engine within the law, if at all. We recognize that this may well mean having to shut down Google.cn, and potentially our offices in China.”

These images below show the difference between Google search results for Tiananmen Square in China and the UK. As is evident, the images of ‘Tank Man’ are omitted. Image 2 (Source: Google.cn and Google.com)
3. The Internet in Iran

Iran has witnessed a rapid growth in Internet usage in the last 15 years, and it continues to increase at a dramatic rate, the highest rate of growth in the Middle East,

“Internet use in Iran was first promoted by the government to provide an alternative means of scientific and technological advancement during the troubled economic period that followed the Iran-Iraq War. Contrary to expectations at the time, the Islamic Republic originally welcomed the Internet by allowing commercial and educational sectors to access it without interference. Whereas in China the technology was largely developed by the state in the form of an intra-governmental communications network, Iran’s first experience with the internet occurred within the university system.” (Rahimi, 2003:102).
Although statistics vary, ONI (2009b) estimates that in 2008, approximately 35 percent of the population of Iran are now online; considering that around 70% of Iranian population is under 30 years of age, prospect for Internet literacy and usage remains high. The Iranian Governments policies regarding the Internet, demonstrate the paradoxical desire to prevent free speech whilst simultaneously harnessing the Internet for economic growth (ONI, 2009b). In October 2006, the government began enforcing restrictions on bandwidth to 128 kilobytes per second, in order to restrict access to multimedia content, although some Universities and Business retain high speed access, “Iran is the only country in the world to have instituted an explicit cap on Internet access speed for households” (ibid). The importance of the Internet in Iran became the focus of much media attention following the infamous elections of 2009 (Ashraf, 2009). Sites such as Youtube and Twitter enabled protesters to document the aggressive and brutal actions of the Iranian Government in attempting to quell the protests. Although the Iranian Government attempted to stifle this avalanche of images and stories, by restricting bandwidth and blocking access, the information was nevertheless able to escape in large quantities and the idea of “one person one reporter” was invented by the Green Movement, the opposition group(ibid).

4. The Internet in China

China now has the highest number of Internet users in the world, some 300 million Internet users, with almost 100 million high speed broadband connections (ONI, 2009a). There is still a digital divide between rural and urban areas in China, but the Chinese Government has implemented policies to further develop Internet infrastructure. Most notably, the Chinese Government has been developing the “Golden Shield Project”, commonly known as the “Great Firewall of China”. This “multimillion dollar Golden Shield project [has] turned the Chinese Internet into Big Brother-net” (Tian, 2006:8). Although it is by no means impenetrable, the ‘Great Firewall’ has allowed the Chinese Government to retain much control over its cyberspace.

5. Internet Filtering

The most comprehensive examinations of censorship and surveillance via traffic analysis in cyberspace have been undertaken by the Open Net Initiative (ONI), who publishes country specific profiles. “Access Denied” (Deibart et al, 2008) published by principle investigators of the Open Net Initiative; Deibart, Palfrey, Rohozinski and Zittrain, details the various methods for analysis of Internet filtering, showing the varying degrees and methods by which states manage and control content. Internet filtering in Iran has been mostly concerned with blocking access to pornography, political blogs and news site such as BBC Persian, Gooyanews.com and VOA Persian service whereas Chinese filters place greater importance on restricting politically sensitive searches, although pornography is also somewhat restricted.
Similar work on Internet filtering has been conducted by Reporters Sans Frontiers (RSF), which aims to encourage freedom of the press and free speech. Their stated goals are to, “defend journalists and media assistants imprisoned or persecuted for doing their job and exposes the mistreatment and torture of them in many countries. Fight against censorship and laws that undermine press freedom” (RSF, 2009).

Iran and China are two of thirteen countries deemed “enemies of the internet” by Reporters Sans Frontiers;

“Iran was among 13 countries branded "enemies of the internet" last month by the human rights group, Reporters Without Borders, which cited state-sanctioned blocking of websites and the widespread intimidation and jailing of bloggers. Critics accuse Iran of using filtering technology to censor more sites than any country apart from China. Until now, targets have been mainly linked to opposition groups or those deemed "immoral" under Iran's Islamic legal code.” (Tait, 2006b)

Julien Pain (2007), head of the Internet Freedom Desk at RSF, shows how dictatorships are becoming more adept at utilising the Internet; whereas in the past the best way to monitor a journalist was to put them under direct surveillance by a police officer, now it is far simpler to use computers to track individuals deemed subversive. An Iranian blogger, Omidreza Mirsayafi, 29, convicted of insulting the Islamic Republic leaders died in jail after taking a drug overdose in March 2009 in the notorious Evin prison; many more are still in prison for having anti government blogs [52, 53].

6. Anonymity – Tor, Incognito, Mixminion and Anonymizer

Various software tools are available to allow users in countries where Internet traffic is monitored to bypass the surveillance operation by hiding the identity of the sender/receiver. In countries that are attempting to restrict and control the internet, the use of proxies and anonymizer tools can help to protect users’ online identity. Proxy servers, gateway applications that are used to route Internet access from within a firewall by opening a socket on the server and allowing the connection to pass through, allow users to protect privacy and remain anonymous (Deibart et al, 2009).

Foremost amongst these software tools is TOR, (www.torproject.org) a free, open source project that uses a network of relays to prevent Internet traffic analysis. Tor is an anonymous communication system that permits its users to surf on the Net without revealing their identity or location. Chaum’s mix-network forms the theoretical foundation for routing used for remaining anonymous on-line, techniques such as onion routing, i.e. a chain of layered intermediary agent relays
Traffic Analysis, Anonymity, Freedom and digital “Cat and Mouse” in Cyberspace: A case study of China vs Iran

(nodes) is set up from the sender to the recipient of a message to hide the identity of the sender [18, 50] The idea is simple, instead of the message taking a known and simple route, the packets travel via a complex maze of relays to avoid trace-route facilities and then to make it harder to be traced, Tor periodically destroying any foot prints along the way. To avoid traffic analysis, anonymity of destination/source is achieved by first distributing the message among participating nodes. The client creates a secure and encrypted path or an encrypted circuit through several Tor relays to a destination. No single Tor relay knows the entire pathway for a cell of data, only the adjacent relays are known whilst extending the circuit one hop at the time; hence hiding the complete path of the source and destination addresses of a data packet.

A directory authority list details of Tor available relays with opinions concerning features such as reliability and fastness. Clients consult this list and based their decision on the consensus. A unique key is issued by the authority such that an attacker cannot convince a Tor user to opt for an un-trusted network [47].

Mixminion uses anonymous remailer protocol and a mix network. Similar to the Tor network, Mixminion relies on donor servers to relay and route your emails from source to their destination. The volunteer servers, called mixes, receive messages, encrypt them with a public key and forward them to the next mix. Effectively, no single mix can determine either the sender or the recipient. All e-mail travel through several mixes so that no single mix can reveal message source with recipients, similar to Tor operation [51].

Incognito is another open source (LiveDistro) free software under the GNU/GPL that is based on Gentoo Linux helps with online anonymity. Incognito works from either a CD or a USB drive and has several Internet applications such as Web browser, IRC client, Mail client, Instant messenger. After rebooting the computer with the CD or USB, Incognito takes control and runs its own operating system instead of your machine operating system [54].

Companies such as Anonymizer.com supply a browser that employs tunnelling technology for creating an encrypted connection with their servers, hence providing anonymous surfing through their proxy. Anonymizer.com software allows your IP address to remain anonymous and is able to encrypt URLs in your browser's history list, however, page titles remain visible. File and digital shredder to clean up hard disk are a good feature of Anonymizer but it cannot handle international file names and javascript code [1].

Although TOR does not guarantee anonymity, it provides an essential service for users in countries where accessing or sending information could prove dangerous. The original goal of Tor was to enhance privacy, recently Tor has become popular amongst users who wish to circumvent national censorship systems, such as those in countries like Iran and China. Tor's primary security property (an attacker cannot find out which websites a user is visiting) also makes it useful for circumvention because the sensor and monitor software are not able to selectively block access to blacklisted sites, Tor does not prevent an attacker from using traffic analysis to de- anonymize users.
Dingledine et al (2010) have attempted to analyse the Tor network, investigating the methods of measuring Tor using client IP addresses and exiting traffic, to counter attempts by some governments to block access and adapt to problems related to Tor's rapid growth. It is however, very difficult to collect data on Tor, without jeopardising users privacy, but also very important in order to keep Tor ahead of potential attacks. The survey used the following principles to protect users when collecting statistics on an anonymity network: legal requirements, user privacy, ethical approval, informed consent and community acceptance. Tor usage significantly increased from Iranian IP space in June 2009 after the infamous Iranian elections. After publishing these statistics, more people were motivated to set up relays and help support the Tor network and Iranian Tor users, in turn improving the security and performance of the network. Such a blocking event has been observed in late September 2009 when China blocked access to most Tor relays. At the same time, bridge usage from Chinese IP addresses increased significantly by a factor of 70 as compared to the time before the blocking. Bridges are Tor relays that are not listed in the public directory, making it harder for the censor to locate and block them.

7. Circumvention

Roberts, Palfrey and Zuckerman, of the Berkman Centre for Internet and Society show the increasing trend towards state surveillance of the internet,

"In the past five years, government filtering of the Internet has become endemic... ...Some states filter just a few websites, such as Singapore; others, such as Iran, filter tens of thousands. China has implemented a vast and complex system which involves filtering international websites as well as pervasive censorship by Chinese Internet companies of content published within the nation". (Roberts, Palfrey and Zuckerman, 2009:3)

They go on to detail the myriad, complex technical solutions that are available and identify the various means by which Internet filtering can be circumvented,

"Some tools (Anonymizer, UltraReach, DynaWeb) use a set of centralized servers as proxies. Other tools (Tor, JAP, Circumventor, Psiphon) rely on peer-to-peer technology to allow volunteers to use their own computers as proxies... Countries that filter the net tend to block access to Internet circumvention tools as well. Anonymizer, for instance, is blocked in most filtered countries. To solve this problem, tools use sophisticated methods to distribute the locations of new proxies, including mailing lists, chat systems and bulletin boards. Peer-to-peer tools like Psiphon rely on their peer-to-peer structure to limit blocking – because very
few people use a given Psiphon node, it is less likely to be blocked. Centralized tools like UltraReach rely on sophisticated anti-blocking technologies to outwit filterers” (Roberts, Palfrey and Zuckerman, 2009:6).

They are quick to point out, however, that none of these solutions is a ‘silver bullet’, describing the government’s filtering strategy as ‘whack-a-mole’ – as one solution to filtering is found, another method emerges. This creates an ‘arms race’ between the governments attempting to censor the Internet and the programmers attempting bypass these restrictions (ibid). A cat and mouse fight on the cyberspace for restricting access by the certain countries and desire for open access by the users and dissidents continues relentlessly. Tim Berners-Lee the inventor of World Wide Web and the World Wide Web Foundation vision is to promote his invention as a tool that supports “democracy and accountable debate”. He stated prophetically that

“Our success will be measured by how well we foster the creativity of our children. Whether future scientists have the tools to cure diseases; whether people, in developed and developing economies alike, can distinguish reliable information from propaganda or commercial chaff; whether the next generation will build systems that support democracy and promote accountable debate, I hope that you will join this global effort to advance the Web to empower people.” [55]

8. Digital Dissent

Ali Batoulli (2004) considers the ‘free Internet’ to be an instrument of state control. Whilst originally setting out to investigate how the Internet can be used as a tool of dissent, he eventually came to the conclusion that the Internet is far more useful as a way of monitoring and controlling civil dissent. Envisioning the struggle between the state and the dissenters as a David and Goliath battle, the Internet provides the critical slingshot enabling a weaker opponent to fell a greater adversary. Unfortunately, this is where the metaphor collapses, as the state (Iran or China) is also armed with this tool, and has better resources with which to utilise it. Batouli concludes

“Those who still believe in the revolutionizing powers of an ever-free Internet are, in a word, idealistic. They choose to ignore the unwanted teachings of experience. They choose to ignore the effectiveness of the State’s power to control its networks through censorship and age-old policing tactics” (Batouli, 2004: 14).

Batouli’s pessimistic attitude towards the Internet as a tool of control has perhaps been borne out by the recent events unfolding in Iran. Batouli
pessimistically writes, “Cyber-dissidents must understand that the Internet is no different than any other tool, be it television or print media; simply put, the regime has more resources, more power, and therefore the advantage... This weapon, the World Wide Web, is only as worldly and wide as regimes such as China and Iran want it to be”. (Batouli, 2004:15).

However, the new digital media has provided dissenters with a wealth of tools, to which governments have been slow to adapt

“The ability of social and digital media to play a crucial role in helping mass social movements coordinate and communicate effectively has been highlighted by the recent post-election unrest in Iran. Due to the borderless nature of digital communications, the resources available to many activists can now be global in scale and supported by virtually instantaneous communication. Some governments have taken notice of this borderless nature and the potential threat it poses. To limit communications within and with the outside world they have erected their own border in the form of firewalls, monitoring mechanisms and internet filtering systems” (Ashraf, 2009).

The talk of a “Twitter Revolution” (Morozov, 2009) in June was short lived. The Internet proved a useful tool initially, to get the message out, organise protests and monitor the demonstrations. However, the state swiftly responded by shutting down access to key sites. Furthermore, it enabled security forces to target individuals involved, and often allowed them to trace an address and location. Using the Internet, in a fashion deemed ‘Immoral’, has become a risky game. Nevertheless, as protests continue, Iranians are still turning to the Internet to help in the struggle against a government that has lost legitimacy in the eyes of many of its citizens. The Iranian government is forced to become ever more violent in dealing with dissent, and images continue to emerge that show police and Basij attacking protesters. In the absence of free press, Internet has been a valuable instrument for oppositions groups and more than 3 million Iranian living outside Iran to link up with their families, friends and political groups inside and outside Iran. An email’s attachment can virtually carry any information undetected; as soon as a site or a blog is filtered, another blog pops up or the filter is bypassed by a code. Mobile technologies have exasperated the situation for totalitarian governments and have added another weapon in the arsenal of the dissidents and political activists. Video clips, photos, sound recordings of demonstration and government atrocities have been broadcasted instantaneously to international agencies. In the case of Iran, digital communication has been advantageous to the opposition groups both in terms of global reach and speed of delivery. In fact the Islamic Republic has been loser in the cyberspace and digital warfare; instead they have resorted to their traditional method of terror and intimidation and shutting
down the Internet, SMS and mobile phones entirely at will. Monopoly of state to control the news and flow of information has been broken.

**Tank Man & Neda – The power of Images**
The success of the Chinese in restricting and maintaining control was epitomised by the PBS documentary ‘Tank Man”, (see Image 3) in which students at Beijing University were shown the iconic image and appeared unfamiliar with it, only hazarding a guess that it may have been a military parade. This shows the extent to which the Chinese government has edited its own history and suppressed information.

*Image 3 (Source: Wikipedia)*

In Iran, the images of the death of Neda Agha-Soltan (See image 4) quickly spread both inside the country and around the world, and have become a symbol of the protests. This shows that despite the best efforts of the Iranian government to stifle and repress information, once an image or idea emerges on the Internet, it cannot be contained.


Meanwhile, China continues to increase measures to monitor and censor the Internet. The dispute with Google in December 2009 has further entrenched the Chinese government who are unwilling to back down. As long as economic growth continues, the evidence from the Chinese citizens’ interviews shows that in general they seem content to be monitored and have content filtered.

**9. Conclusions**

Despite some similarities between the two government’s methods of controlling cyberspace, the attitudes of the Chinese and Iranian citizens regarding this trend differed greatly. A return to the theoretical framework of Foucault’s (1977) Panopticon will help understand and explain this discrepancy.

The aim of the Panopticon is

>“to induce in the inmate a state of conscious and permanent visibility that assures the automatic
functioning of power \[\text{and to produce}\] homogeneous
effects of power” (Foucault, 1977:201)

As Tsui (2003) states, “China has the perfect ingredients ready for a digital
Panopticon” (Tsui, 2003:44). The Chinese government has been incredibly
successful in creating a society in which the state not only controls cyberspace, but
also uses it as a tool for reinforcing control. From the interviews with Chinese
citizens it was clear that although they were aware of the censorship and
surveillance, most were unconcerned, even considering it normal.

In contrast, the Iranian citizens interviewed were extremely unhappy with the
increasing trend towards censorship and surveillance within Iran. The fact that the
Iranian government has been slower than China in enforcing its control over
cyberspace, has allowed it to grow into a space of virtual resistance (Batoulli,
2004). The Persian/Iranian blogosphere has become an essential outlet in a society
where strict moral codes are enforced by religious police (Rigby, 2007). The rapid
growth of blogging in Iran has created a strong online community with an outlet to
express dissatisfaction. Attempts by the Iranian government to stifle this space of
free expression have only led to further disaffection (Ashraf, 2009).

Therefore in summation, the communist government of China has been more
successful in creating a panoptic state due to a number of factors: 60 years of strict
communist rule resulting in a culture accepting of one party rule. The controlled
economic freedom of the last 20 years resulting in overall growth and relatively
higher standard of living for new generations compared with their parents. A
perceived expectation that through, education, work and faith in the government
policies, a brighter future can be achieved. Increasing prestige, power, and
influence of China in the world and its ascendancy to the present second super
power status and an early awareness of the need to restrict the freedom and take
control of Cyberspace.

In contrast, the failure of Iran to gain control of cyberspace can be attributed to its
political and social turmoil in the past three decades, poor IT infra structure,
meagre e-commerce activities, and minor level of IT/Internet literacy among the
ruling clergy. The late, gradual and crude attempts of the Islamic Republic to
restrict freedom in cyberspace propagated the growth of a vibrant blogging
community, but stifled economic growth and resulted in the loss of international
sympathy and encouraged the recent UN sanctions [56].

In the aftermath of the 2009 election, the power of the Internet as a place of
resistance and tool of opposition became increasingly important (Ashraf, 2009).

Efforts by the Iranian government to counter the threat posed by the Internet
involved shutting down entire networks, not a practical solution in the long term.
Indeed, this was a vindication that Iran is not reliant on the use of technology for
managing its social and economic wellbeing. In contrast to china, traditional
commerce (Bazaar) and state controlled industries such as gas and oil are the
powerhouse behind the exhausted Iranian economy.

That said, the panoptic nature of the Internet has allowed the Iranian government to
target dissenters and arrest protesters (Morozov, 2009). Nevertheless, the
government has been unable to contain the flow of information, stories and images
that have emerged in the aftermath of the election, none more poignant than that of
Neda Agha-Soltan. The footage of a young girl shot and killed on the 20th of June
2009 quickly spread both within in Iran and to the rest of the world, and has become an iconic symbol of resistance. As is evident from the reaction of the Iranian government to the protests, Foucault’s idealistic hopes for the Islamic Republic have not been realised. However, when Foucault talks of the using the tools of modernity (radio broadcasts and cassettes) as means of resistance. The protesters, in their use of the Internet have mirrored this utilisation of technology for resistance (Afray and Anderson, 2005).

The disciplinary power of the state is greater in China than Iran – as demonstrated by the recent protests. Furthermore, a successful disciplinary society does not need to utilise what Foucault (1977) terms ‘spectacle’ to emphasize its control. Iran still practices public hangings, flogging, stoning and direct, visible demonstrations of force and punishment in order to maintain control. In China, these methods are unnecessary and in extreme cases dissenters are more likely to disappear.

Therefore, while China has succeeded in creating a Panoptic state, Iran has reacted too late to contain online dissent. The Islamic Republic has so far managed to retain control, through force, but the voices of opposition are growing online, and spilling out into protests and actions on the streets.

More recent developments on this issue have shown that Google may be forced to acquiesce to the demands of the Chinese government in order to renew its ICP license. As long as economic growth continues, the evidence from the Chinese citizens interviewed shows that in general they seem content to be monitored and have content filtered.

While both Iran and China remain committed to maintaining control over the digital technologies available to their citizens, restricting cyberspace and continuing to play this digital ‘cat-and-mouse’ game with dissenters, services such as Tor, Mixminion, Incognito and Anonymizer play a vital role in protecting the anonymity of their users and preventing the hegemonic control that these authoritarian states would like to impose on their citizens. The demand for Tor has increased in recent years which mean network loading has gone up significantly. However, the rate of donation of relay servers to match this demand has been slow and has adverse effects on load balancing and performance [50]. Although it may be difficult to gain an accurate picture of how many individuals are utilising these anonymity tools and for what purposes, it is clear that they provide a vital service, bypassing restrictions and concealing online identities.

The inherent robust architecture of the Internet and its associated protocols and routing algorithms designed for survivability and message delivery in case of all out attack, makes it harder for both sides to win outright in this digital cat and mouse game of cyberspace.
10. References

17. Geelkerken F.W.J. van (2008), Egregious use of Tor Servers? Data retention, anonymity, and privacy on-line, CFET, Canterbury, Kent, UK
31. Karsten Loesing1, Steven J. Murdoch, and Roger Dingledine ; The Tor Project “A Case Study on Measuring Statistical Data in the Tor Anonymity Network” Computer Laboratory, University of Cambridge, UK
36. Rahimi, B. 2003: Cyberdissent: The Internet in Revolutionary Iran. Middle East Review of International Affairs. 7: 3: 2003
42. Tait, R. 2006b. ‘Censorship fears rise as Iran blocks access to top websites’. The Guardian (Online) 4 December. http://www.guardian.co.uk/iran/story/0,,1963166,00.html [Accessed 6 August 2007].
44. Tsuen-Wan “Johnny” Ngan1, Roger Dingledine2, and Dan S. Wallach; Building Incentives into Tor; 1 Google Inc. 2 The Tor Project; Department of Computer Science, Rice University
47. On Anonymity in an Electronic Society:
50. Wan Tsuen-“Johnny” Ngan1, Roger Dingledine2, and Dan S. Wallach3 Building Incentives into Tor ;Google Inc.; The Tor Project; Department of Computer Science, Rice University