ECIPE OCCASIONAL PAPER • No. 5/2011

DIGITAL AUTHORITARIANISM:
Human Rights, Geopolitics and Commerce

By Fredrik Erixon and Hosuk Lee-Makiyama

Fredrik Erixon (fredrik.erixon@ecipe.org) and Hosuk Lee-Makiyama (hosuk.lee-makiyama@ecipe.org) are Directors of the European Centre for International Political Economy (ECIPE)

www.ecipe.org

info@ecipe.org Rue Belliard 4-6, 1040 Brussels, Belgium Phone +32 (0)2 289 1350

EXECUTIVE SUMMARY

Online censorship is about to take centre stage in the campaign to improve conditions for human rights, cyber security and commercial freedom of exchange on the Internet. Online censorship may be a recent phenomenon, but censorship is not. Yet the extent and impact of censorship has taken new forms, in some instances reached new heights, with the progressive spread of new communication technologies. Censorship and authoritarian control of the Internet has a cascading effect, impinging on national security, external relations with foreign powers, human rights and commerce.

Governments in authoritarian regimes have been remarkably successful at adapting to the perceived dangers posed to their political authority by the Internet. China is a case in point. While it promotes its usage to benefit economic growth and industrial development, the Chinese Communist Party has also turned the Internet into a tool to control and maintain political stability. This is reflected in the increase in Internet-related arrests. An increased use of cyber espionage and military development has helped to further China's foreign policy goals and increased geopolitical leverage abroad.

In hindsight, the early hopes that the Internet would quickly usher in a wave of new pluralist political reforms in authoritarian countries like China now appear naïve. It has yet to happen. It may, however, happen in future, and it is incorrect to assert, as some do, that the Internet will never be a catalyst in reforming the Chinese political system. But for the moment digital authoritarianism has the upper hand over digital liberation.

The view this paper purports is that foreign actors can help to redress this imbalance by taking China to the WTO for flaunting its commitments. Principally, a WTO case against online censorship could not attack the entire system of censorship in China or any other country. China, and possibly also other countries, is in violation of its WTO commitments *when it uses censorship as a tool of discrimination and when its censorship actions are disproportionate to the stated aim of the actions*. Hence, the economic rights of other countries get violated by actions to censor the Internet and online communications.

Naturally, it is not all censorship actions that violate the rights of other countries; hence, a WTO case is not a strategy to address all problems caused by censorship. But important parts of censorship do violate economic rights. And as has been shown in past WTO cases of principal interest, it is possible to get a country like China to behave in better ways when countries defend their economic rights. Such an outcome would benefit freedom of expression and the efforts to combat cyber warfare.

1. INTRODUCTION*

Online censorship is about to take centre stage in the campaign to improve conditions for human rights, cyber security and commercial freedom of exchange on the Internet. Online censorship may be a recent phenomenon, but censorship is not. It dates many centuries back, and has been, for short or long periods, a restriction on the freedom of expression in most parts of the world. Yet the extent and impact of censorship has taken new forms, in some instances reached new heights, with the progressive spread of new communication technologies. Recent events –the successful "Facebook" revolutions in Tunisia and Egypt; curbing of the "twitter revolution" in Iran, or Google's decision to no longer run its China-based version of the search engine – demonstrate that the effects of censorship extend beyond national borders, and that censorship affects more than just the flow of information and media. Censorship and authoritarian control of the Internet has a cascading effect, impinging on national security, external relations with foreign powers, human rights and commerce.

While many countries in the world apply some form of censorship, there is one country that really stands out, both for the coverage and the strictness of enforcement – namely China. What is further complicating online censorship in China, and outside reactions to it, is that the country now is the largest Internet market in the world, if one measures it in terms of users. The number of Internet users in China outgrew in 2008 the number of users in the United States. Moreover, the number is growing rapidly and amounted, according to a survey in mid 2010 to 420 million users.[1]

While the United States, and to some extent other Western nations, may still lead the technological development and commercialization on the Internet, developing or emerging economies such as India and China, are now increasingly reshaping the Internet, its usage, regulation and role in society. It is also the emerging economies that have pushed the transition of Internet usage to mobile and wireless networks. As the world is inexorably shifting eastwards, with a growing influence in the world's online retail markets for countries like China and India, it should be clear to everyone that their role in the design of rules and policies governing the Internet will increase and affect the way Western countries approach these issues too.

This paper stands at the nexus of the Internet and global politics, and especially the growing role played by some of the emerging economies in shaping, by accident or design, Internet governance. More precisely, the paper concerns the use of online censorship practices by principally emerging countries and how they affect domestic conditions, like the freedom of expression and political pluralism, and foreign countries in their strive to increase the role played by the Internet for political and commercial freedoms. Furthermore, as societies grow more dependent on the Internet, online censorship also ventures into affairs of cyber security. The paper aims to shed light on the effects of online censorship for cross-border commerce, human rights and cyber security.

The view this paper purports is that these concerns "hang together". There is little use – intellectually and strategically – to make them opponents, by asserting, for instance, that the presence by foreign online companies in authoritarian regimes as a general rule undermines foreign calls for human rights improvements. Even if there are such examples, the larger problem is that when human rights get violated the same action typically tramples on freedom of commerce. The flipside of the coin, however, is that improvements in commercial freedoms online can improve conditions for online freedom of expression.

* The authors gratefully acknowledge the able research assistance of Mr Mark Willis

Finally, the paper will discuss how other countries can respond to the growing problems caused by online censorship, principally through external commercial policy. Undoubtedly, this paper can be accused of being too narrowly focused on trade policy as an avenue to improve online freedom of expression. We accept that critique. But apart from the odd paper[2] and political statement from European Union leaders[3], the commercial policy avenue for restraining online censorship has been neglected and unexplored. There is also confusion among many people who discuss and refute that option. It is therefore important to increase understanding about how trade policy, and especially trade law, could be used to constrain the discretionary use of online censorship by certain governments.

2. PRACTICE OF ONLINE CENSORSHIP

Censorship going online

Online censorship is no different from traditional censorship as far as its purpose is concerned. Controlling political dissent, allegedly to protect societal and political stability, is the most common reason for governments to restrict their citizens from freely expressing their views. But censorship stretches beyond that motivation. This is not to say that all forms of censorship are related and equally disturbing; on the contrary, it is to give examples of the wide variety of motivations for censorship, some of which are, by themselves or the political process that led to them, democratically legitimate while others are not.

The rationale that is most commonly referred to is political censorship and for monopoly of power. Vietnam, China and certain countries of the Persian Gulf (Iran, United Arab Emirates and Saudi Arabia to name just a few) enforce censorship by blocking offensive content at home and abroad in order to maintain the status quo and single party or family regimes. Past regimes in Tunisia and Egypt were also examples of this. A particular variation of this is *lèse majesté*, the crime of criticising or insulting the head of state. The Turkish courts banned YouTube, partly because of content deemed offensive to the memory of Mustafa Kemal Attaturk, the founder of modern post-Ottoman Turkey. A similar block of YouTube has also occurred in Thailand, where a derogatory text message about the King between only two private parties resulted in an arrest.[4] Allegedly, placing another image above the portrait of the King on a web page is enough to generate a complaint.[5] Censorship based on religious concerns is also common, especially in the Muslim world on activities relating to pornography and gambling. The Pakistan Telecommunications Authority banned access to Facebook citing concerns over 'growing sacrilegious content' in May 2010, and censorship over blasphemous content has also escalated following the controversial Danish cartoons of Prophet Muhammad in 2006.

However, censorship is not limited to religious objectives or authoritarian societies – in fact few, if any, liberal democracies have absolute unrestricted access to the Internet. Most societies apply blocks on child pornography or other kinds of illegal content. South Korea filters online content for national security against content that support North Korea. Furthermore, many European countries (including Germany and France) have outlawed glorification of Nazism, and even the United States has banned online gambling. However, these restrictions tend to be legal bans (although it may be applied ex-territorially)[6], rather than technical filters that restrict access altogether. Currently, there are now over forty countries involved in physically restricting information flow on the Internet, compared to only a handful ten years ago.[7]

Why online censorship in China is different – and why it matters

Online censorship varies in purpose, form and extent, but nowhere is it as advanced and comprehensive as in China.[8] It is also the country whose online censorship is causing the greatest damage – on individual as well as commercial freedom.

At home - within China's own jurisdiction - the government can request the removal of any information at any time at the source. This is achieved through the requirement for all website owners to hold a state licence (a so called ICP-licence or Internet Content Provider licence) and make them legally responsible for all published content, and through rigorous "self discipline" demanded by Internet service providers and Internet cafés which make sure that unauthorised information remains blocked. Forbidden topics and words are listed in a black list circulated in media and service operators, which also affect text messages (SMS) and mobile applications. In times of heightened tension, the government even shut down all communication in specific locations so that citizens cannot use the Internet or mobile phones. Such an extreme case occurred in China's Xinjiang province where, after the ethnic riots in July 2009, the Internet was cut off in the entire province for ten months.[9]

China's authorities act even more severely against information and websites based abroad. All entry ports to the country go through state-run operators and a firewall known as "the Great Firewall of China" in the west and "the Golden Shield" in China, blocking access to at least 18,000 foreign websites.[10] The government have blocked various political organisations and popular foreign news media like the BBC and the New York Times, especially during times of heightened political tension. User-generated content sites like YouTube, Flickr, and blogs like Blogger, Wordpress and LiveJournal are still either entirely or repeatedly blocked, as are social networking sites like Facebook. As we will see, an assortment of domestically bred online services has cropped up to replace these services in China that are now raising capital abroad and eyeing exporting their services.[11] In conclusion, China maintains today the most technologically advanced form of online censorship. Worryingly, China is a trail-blazer and one of the leading exporters of regulatory order for the Internet. Its techniques are increasingly copied and adopted by other countries. And as the world's largest Internet population, no other country, bar the United States, carries same weight in defining the future of the Internet.

3. DIGITAL HUMAN RIGHTS

Development of liberties and modernisation

Online censorship violates a fundamental human right: the freedom of expression. Such abuses have been well documented in Western media, with many NGO groups such as Amnesty International and Human Rights Watch throwing light on this dark art and drawing public attention to individual examples of cyber dissidence. Human rights groups have also sought to influence public opinion and pressure multinational corporations with established businesses in authoritarian regimes to restrict or close their economic activities. Some even herald the notion that the technological upgrade in authoritarian societies have entrenched rather than diluted the ability of autocratic regimes to maintain their monopoly on political power. This may be a minority view, but it is echoed in the disappointment many feel over the failure of the Internet and the ICT revolution to dismantle oppressive regimes. Ten or fifteen years ago, the consensus of the commentariat was that oppressive regimes would never be

able to control opposition and censor dissenting views online. Grand theories were built on that promise. The pendulum has now swung – not to the opposite extreme, perhaps, but at least into the opposite camp.

The persistence of autocracy and stymied freedoms in a country like China has provoked some observers to revaluate the old modernisation theory and suggest there is a disconnect between increasing economic freedom and Internet availability, on the one hand, and maintained – or even heightened – suppression of political freedoms and human rights, on the other hand. It has been the core element of the modernisation theory for a long time that economic modernisation will give birth to political modernisation: economic liberalism will foster political liberalism. In this somewhat Marxian, or materialist, view of history, economic development will feed political reforms by changing the "habits of the heart" of elites and people, and making old repressive structures an enemy of continued prosperity. An alternative version, based upon Tocquevillian political thought, is that economic development will form a broad middle class that will demand political representation and civil liberties.

This theory of development can find empirical support. After all, this has been the taxonomy of development in many countries that during the nineteenth and twentieth century moved from economic and political underdevelopment to become advanced democratic market economies. Fast risers in Asia such as the Asian Tigers broadly followed this path to the open society. However, noted scholars as Minxin Pei and Fareed Zakaria have in recent years floated scepticism towards this supposition of a clean, arithmetic and inevitable link between economic modernisation and democracy.[12] Many have argued that a country like China, and possibly others too, has rather put a different model of modernisation on the table: *developmental autocracy* or *developmental authoritarianism*. A soft version of this school of thought suggests there is only a tenuous relation between economic and political modernisation. A harder version rather emphasises the role of economic modernisation for *maintained* suppression of political freedoms and human rights. In China, for instance, this view holds that the long wave of economic modernisation, and the ensuing growth, has helped the ruling party to maintain its grip on power.

There are inarguably some merits to this view. But they are neither new nor reasons to refute the modernisation theory lock, stock and barrel. Certainly, there is no automatism in the modernisation of society, and the supposition that political modernisation will inevitably follow hard on the heels of economic modernisation is false. Economic modernisation often gives increased power to groups in favour of political reforms, but such reforms have never come without people fighting for it – more often than not over a long period of time. It is also true that some countries have followed the opposite track with partial political and civil freedom reforms preceding reforms to modernise the economy. This is what happened in many Western societies where some civil liberties (freedom of expression, press freedom, et cetera) took root before periods of economic modernisation.[13]

There is room for scepticism of the modernisation theory, especially its asserted inevitability or what some see as monopolistic aspirations (not accepting alternative or even complementary theories of change). Yet it is hardly correct to say economic modernisation will not have a positive influence on political modernisation. Even today's China shows there is a positive correlation. China is a much more open society today than it was in the 1990s, let alone in its dark age before the grand opening up in the late 1970s. The room for expressing views, including dissenting views, in China has increased, even significantly so, over the past decades. For anyone who experienced China in the 1980s or early 1990s, the current atmosphere is

better by almost any comparison. In the period up to the Tiananmen Square horrors, the climate of opinion was invigorated with a broad and vibrant democracy movement, supported by newspapers and many CCP officials, even the General Secretary, Zhao Ziyang, who was forced out of office and into long house arrest due to his support of the demonstrating students in Beijing. At the time, many people felt China was on the eve of democratic reforms. But that hope, and the general move towards openness, was brutally crushed by tanks on June 4, 1989. Heightened oppression followed, with Beijing being nervous of any sign of public dissent with the party. The climate, however, has improved since the post-Tiananmen period. There is now inarguably a greater degree of openness.

Diversity under control

THIS OPENNESS HAS inarguably created a vivid and active online community in China. Just to take one example, there are over 70 million blogs in the country.[14] Chinese Internet users are now spending more time online and on social networking sites and chat rooms than users in other parts of the world (except France and South Korea). This huge increase in popularity of direct online communication, especially through online forums, has created an arena to voice dissent and express opinions to a wide audience anonymously. A recent academic study in the journal *Asia Survey* found that a clear majority of the studied blogs in China (61%) presented "critical" opinions of the government, corporations, and public figures, while 36% of blogs expressed "pluralist" perspectives.[15] The Chinese authorities have responded by requiring bloggers and forum participants to provide identification. But despite such measures, there is a clear trend that China's bloggers and online chatters express their critical views more openly, and the overall pattern is that citizens express critical views more often now than before the "Internet revolution" within the thresholds of what China's ruling party allow. The Internet has played a marked role in diversifying the public debate, opening up new avenues for citizens to sidestep traditional media, which is often state controlled and reports the official viewpoint of the state. Similar experiences have been noted in the Middle East and elsewhere in the world.

The growing use of Internet in China is indeed a challenge to China's ruling Communist Party (CCP). It has devised a comprehensive strategy to combat any challenge by censorship and strong state control over the Internet and media. This strategy was recently affirmed by a White Paper from the China State Council, making clear that laws and practices are not about to change.[16] The 2010 Nobel Peace Prize winner Liu Xiabo highlights the fact that there are certain views that simply cannot be expressed publicly in China without punishment from authorities. Limitations to access and expression of ideas do not only violate the rights of the citizens, but also those of journalists, media outlets and their right to express ideas and commercialise them. One example of how the Internet has enabled authorities to control and disseminate information is how governments are able to restrict the news flow and often publicise its version of a news story first. China, for instance, often employs commentators to "guide" public opinion. China's Internet Affairs Bureau sends out strict daily instructions regarding the manner in which large news websites should cover specific events or incidents, how websites should highlight or suppress certain type of opinions or information – all in a very detailed manner. The most recent example of such restrictions is the Jasmine revolutions in North Africa. News reporting was gradually restricted in China and calls for protests at home on Chinese micro-blogging sites and text messaging to multiple recipients were stopped.[17] China has even attempted to ensure state monopoly on financial news,[18] and the media were forbidden to mention any ideas that US pressure may be contributing to Chinese

monetary policy. Online reporting on strictly domestic affairs, such as a stabbing incident in a kindergarten in Zheng County in May 2010 was restricted from being placed prominently and with user comments disabled.[19]

It is therefore barely a surprise that Reporters without Borders ranked China in its Index of Press Freedom at 171th out of 178 countries with 30 Chinese journalists being detained or imprisoned for "inciting subversion" and "revealing state secrets". Only countries like Eritrea, North Korea, Iran and Burma are considered to have worse conditions for journalists.[20] But increasingly, bloggers and online commentators also face the threat of arrest, and the number of imprisoned "netizens" is now 78.[21] Internet also has increased the dispersal of government information and the government's surveillance capabilities. For example, by targeting certain types of Internet activities like Bulletin Board Systems (BBS) and forums, authorities have been able to seek, identify, and suppress citizen dissent. Sauce for the goose is sauce for the gander, to put it cynically. If people express dissent openly on the Internet, it is also possible for censors and the machinery of thought control to read it.

It is clear that the ever-stricter enforcement of China's censorship has slowed down the trend towards democracy and civil liberties. Some will call this a failure on the part of the Internet – or at least a failure by the Internet evangelists to deliver on the promise of inevitable freedom and democracy. That is unfair but it illustrates how rigorous and widespread censorship governance has become that authorities manage to sufficiently control the dissemination of opinions that are deemed too critical of the government. Those who advocate authoritarian control of Internet often argue that Chinese online censorship enjoys popular support: a frequently quoted study published by a U.S. think tank (but carried out by the Chinese Academy of Social Sciences) concluded that 80 per cent of respondents felt it necessary to control the Internet and 41 per cent believed political content should be restricted.[22] Furthermore, 85 per cent of the respondents felt it is the government who should assume the role of managing and controlling the Internet. Now, 41 per cent is not a resounding majority. Nor can the study itself be considered evidence that Chinese people have faith in the censorship regime. The term *censorship* was actually not mentioned in the questionnaire – and a similarly phrased survey question asking whether the Internet should be managed or controlled to a certain extent could conceivably produce a similar response in any democratic society. Simply, many people agree that there should be *some level* of regulation without specifying whether they should go beyond those applied in western democracies.

As we have seen, there is an increasing list of countries that are following Chinese practices. But what is also worrying is how Western countries are treading this path, albeit in a very different way than in China. One example is how Italy obliges Internet Service Providers (ISPs) to block access to certain sites without any court issuing such an order. There is an increasing pressure on regulating the Internet and an increasing number of countries appear to accept trespassing on civil liberties as a "price to pay" for regulations to be operable. These trends should alarm political leaders in the West and caution them against going down the road of online censorship, especially as measures would have never been accepted if it had concerned censorship of printed media. That would in itself be bad policy – but it would also lend legitimacy to censorship in authoritarian countries that carefully watches developments in other countries. A representative of the European Union voicing critique against China's online censorship, while supporting some forms of online censorship at home, will be considered as hypocritical by a Beijing that has mastered the skill of downplaying its own vices by comparing them with the vices of others. Never mind the profound differences in civil liberties, China will accuse "the West" of using double standards: one benchmark for

China, another for the West. This is not a distant speculation – it has already happened.

Means of addressing online human rights issues

As the role played by the Internet and digital sector in the lives of individuals, governments and businesses has increased, it is inevitable that the unrestricted freedom to use this medium for information exchange has rightly come to be seen as a basic 21st century human right. However, billions of people around the world are denied that freedom. In 2010, using unusually blunt and critical language, the US Secretary of State, Hilary Clinton, called China's censorship regime as an 'Information curtain'.[23] The Swedish Foreign Minister, Carl Bildt, has expressed similar views, drawing parallels between the firewall in China and the Berlin Wall.[24] These are two examples of a promising new trend: political leaders are becoming more vociferous about online censorship and its menacing effects.

Although human rights have existed in various legal systems, universal human rights in international law are a novelty. They were established at the end of World War II when the United Nations Charter committed all members to fundamental human rights and freedoms without distinction as to race, sex, language or religion. It also adopted the Universal Declaration of Human Rights. From the examples above, it is clear that several rights in the declaration are inarguably violated – primarily article 19 on freedom of expression. However, the UN system is a politicised forum whose track record has proven to be ineffective in addressing human rights issues against another UN member. Compliance with the Charter and the Universal Declaration is not independently measured; it is negotiated between members – some of whom believe in human rights while some do not. Due to its composition, the UN Human Rights Council has been incapable of taking any form of action against human rights violations. The same verdict goes for many UN bodies, including the Internet Governance Forum (IGF), or the World Summit on the Information Society (WSIS) that created it in 2003 for the purpose of assisting the United Nations on Internet governance as a forum where governments, businesses, and stakeholders could discuss issues related to the deployment of the Internet, including upholding the Universal Declaration. Perhaps due to the inherent limitations, the multilateral system under the UN remains a forum for exchanging views and experiences (albeit useful for that purpose) rather than rule-based bodies to address human rights violations.

Another way to fight human rights violations over the Internet has been to take unilateral action by obliging home firms operating in authoritarian countries to depart or in other ways change. Such proposals present a moral dilemma for companies. Some have favoured disengagement from such countries – even if their dismemberment will have no effect on censorship itself. Several EU and US firms have been criticised for supplying telecommunication equipment to totalitarian countries like Iran and Belarus although the delivered equipment is identical to the ones supplied to markets in Europe and the US. The European Council has explored the means of unilateral sanctions that include telecommunication tools, while certain members of the US Congress have sought to solve this dilemma by initiating a "Global Online Freedom Act" where businesses co-operating with 'authoritarian foreign governments' would be penalised.[25] The problem with such policies, however, is that their efficiency is at best limited. At worst, such measures could be counterproductive. Few countries would be pressured to change their behaviour because of a threat that a foreign firm may have to depart. The service or good provided can in most cases be purchased elsewhere, perhaps even domestically. The departure of foreign firms is also likely to have a depressing effect on the small interest of an authoritarian regime to behave better. Departures and other symbolic

moves on the part of one company can become an obstruction to other companies operating there. The effect could be a double whammy: it damages firms and withdraws liberating technologies from foreign citizens living under oppression.

While many NGOs still demand such unilateral withdrawal, the policy responses by the EU and the US seem to largely embrace the notion that businesses providing technologies is a positive force for change, outweighing the problems associated with operating in authoritarian regimes. 'Digital diplomacy' and Internet freedom have been elevated to a central pillar of State Department's policy under Hillary Clinton, and market actors in the digital economy play a significant role in it.[26] Similarly, the European Union has made securing Internet access a part of its new strategy for the southern Mediterranean region.[27] So the question is how, and not if, online issue should addressed by policy makers.

Addressing the topic as a human rights issue has rendered few results. In some instances this strategy has even backfired. The US State Department enthusiastically endorsed a circumvention program called Haystack which turned out to be ineffective, at best, and possibly even counterproductive by unintentionally leaking user information to the oppressing regimes.[28] Governments in general (but diplomats in particular) seem to be ill suited to making technical decisions on how to protect the highly innovative and internationalised ICT sector and its market driven actors, such as Twitter, Google or mobile network operators. Appropriate and feasible policy responses do not seem to be multilateral and unilateral enforcement of human rights, technical capacity building or development aid – defending online freedom and technologies that enable them must be implemented in other areas of foreign policy.

4. NEW PARADIGMS OF SECURITY

New capabilities, new threats to open societies

In November 2010, it was reported that a computer worm called Stuxnet had infected several controller equipment designed for use in industrial automation all over the world. While it did little or no harm to the systems, except instructing them to spread the worm further along the network, it allegedly caused the processing units in Iranian nuclear facilities in Bushehr and Natanz to spin out of control and self-destruct. While the actual origin of Stuxnet is still unknown, there is less doubt about its target – most likely, the worm was a targeted attack against the Iranian nuclear program, and was meticulously designed to affect only its target.

Cyber warfare has rapidly established itself as the new theatre of war. It is, especially in the eyes of some military hawks, the fifth realm of war following war on land, sea, air and the recent militarisation of space. One of the earliest incidents of an outright war (as one state attacking another online) occurred as recently as May 2007. After a tense diplomatic standoff between Russia and Estonia, websites of Estonian political parties, government, banks, and media were disabled by a three week bombardment of Internet attacks, many of which are thought to have originated from state-sponsored Russian hackers (though this was never proven). Estonia, one of the pioneers of e-government, is heavily dependent on the Internet for its day-to-day functioning and the 2007 Russian attacks showed how much damage well-targeted cyber warfare can inflict on strategically important targets.

Despite its short history, cyber warfare and terrorism have become the main pre-occupation of military and civil security agencies the world over. The United States has established a command structure for cyber defence under a four-star general, and defending information and communication is now a part of the strategic concept of NATO.[29] There are plenty of

voices that point to the need for improving capabilities in this new branch of arms, including the former US anti-terrorist czar, Richard A Clarke. Others include the Director of the United States Central Intelligence Agency, Leon Panetta, who in April 2010, claimed that "The next Pearl Harbor is likely to be a cyber attack going after our grid",[30] which followed an earlier warning from Dennis Blair, a recent Director of National Intelligence, that "attacks against networks that control the critical infrastructure in this country could wreak havoc".[31] Even President Obama has made that abundantly clear when he launched the cyber-security initiative in late May 2009 by admitting that the United States was not "that prepared" for a attack, and it would have been ridiculous to suggest anything else.[32]

Regardless of whether there are real risks for war or not, these warnings express an anxiety that an increasing number of policymakers now are starting to understand – the vulnerability of modern connected societies. A special Commission on cyber security, housed at the Center for Strategic and International Studies in Washington, DC, released a report in late 2008 which bluntly stated, "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration".[33] This conclusion was echoed in early 2010 in a study by the Bipartisan Policy Centre which simulated cyber attacks on the United States and examined how the government would develop a real-time response to a large-scale cyber crisis.[34] The simulated attack aimed to recreate a situation where US mobile phone networks, power grids and an electronic energy-trading platform were severely damaged by a malware program that had been planted in phones months earlier. The study concluded that "Cyber attack poses a genuine threat to US national security and that the government should deploy more resources to defence measures against such attacks".[35]

Other countries, too, have been slow to react to this new theatre of war. The European Union, for instance, has no common policy for cyber security. The EU Strategy for a Secure Information Society from 2006 addresses only Internet-based crimes, and the European Security Strategy, adopted by the Council in December 2003, makes no reference at all to cyber security.[36] And a follow-up, implementation document for the security strategy only addresses cyber security concerns by saying "More work is required in this area, to explore a comprehensive EU approach, raise awareness and enhance international co-operation."[37]

Threats against civil security

It is clear that "the grid" that Panetta and others talk about has a wider meaning than in the past. Fifty years ago, strategic civil defence planning involved food and energy supplies (countries deliberately designed autarkic production systems in these sectors for reasons of contingency planning), transportation infrastructure (roads, railroads, airports and ports) to maintain structures for command and public management. Civil security is very different today as open and modern societies rely on several layers of subsidiary and auxiliary networks in order to make the most basic necessities run: banking and financial systems are entirely dependent on electronic communication; in most countries, traffic monitoring systems are run by advanced IT systems; public broadcasting is no longer transmitted through air but triple play and IP networks. The interdependency between various layers of governance and the economy is stronger than ever. This vulnerability poses a new challenge for civil security, and has fundamentally redefined the risk beyond physical threats and some of the most dangerous threats today are virtual.

Some important political implications emerge from these new risks. It has 'levelled the playing field' between activist groups or states unable to match the military capabilities of NATO

or the US. Many of the noted attacks are small scale, by unknown groups with limited means. For example, Microsoft documents were used in an alleged attempt to install spyware into the German Federal Chancellery, the Foreign Office and other government ministries, and although there are suspicions of some state involvement, it was performed by individuals using very few resources.[38] The identity, motives and political agenda of such groups are often unclear. They do not necessarily have to be sympathetic to one or several political causes – but can nevertheless cause serious damage to international relations.

In the German example, suspicions were pointed at a group based in China, which raised broader questions about the future of German-Sino diplomatic relations.[39] Similarly, China-India relations took another dive recently when a cyber attack against Indian national security authorities was suspected to be originating from Chengdu (the capital city of the Sichuan Province in China). It did not appear as if the perpetrators had any political motives, and the Chinese government firmly denied any involvement, but it nevertheless increased tensions between two nuclear states with longstanding border issues between each other.

Is cyber warfare really about wars? So far incidences have mostly been asymmetrical conflicts staged by non-state actors that exploit the vulnerability of modern societies – be it political offices in Germany, or nuclear centrifuges in Iran. Cyber terrorism or espionage is a better term for such actions than war. Moreover, cyber defence capabilities in the EU and the US are by and large non-existent, and this is perhaps because cyber warfare is an offensive capability, not a defensive one. As with terrorism and other asymmetrical threats, there are few means of deterrence against cyber attacks. Against whom would Germany and Iran retaliate? The lack of defensive measures available is revealed by another attempted attack against US National Security Agency, which was made through a simple USB thumb drive. [40] The key policy response by the agency was to seal all ports on their computers with liquid cement. Unplugging the net seems to have been the general policy response to the new threats. While the Internet was founded on principle of decentralised, interconnected and open networks, it is increasingly becoming fragmented along the national borders, and it is today possible to talk of several *Internets*, in plural. Language barriers and industrial policy also spur the process of balkanisation – in fact, the Internet in China, India and the United States look very different already. But geopolitical concerns are increasingly important factors for this fragmentation: Saudi Arabia and the United Arab Emirates threatened to ban Blackberry handsets unless user data was stored on servers placed on their territories.[41] Google felt compelled to leave China once it refused to engage in censorship, and after it had found that hackers had stolen proprietary information data (together with companies in surprisingly non-strategic sectors like finance and chemicals) and email accounts belonging to Chinese dissidents had been hacked.[42] China has in turn introduced Multi Level Protection Scheme (MLPS) to limit the possibility for non-Chinese firms to deliver critical infrastructural services and goods.[43] In response, the US Committee on Foreign Investment in US (Cfius) has barred Huawei and other Chinese telecommunication firms from making acquisitions in the US.[44]

5. BUSINESS – A CASUALTY OF CENSORSHIP AND CYBER WARFARE

Authorities are generally capable of upholding traditional structures and societal necessities – such as fuels, maritime shipping or postal and courier services – in the event of war. Yet they are unable to protect equivalent structures for information technology. One key difference between cyber and traditional warfare is that private business is in the line of fire to a much greater degree in the former type of warfare. Non-state actors often are at the centre

of this new theatre of war. Some of them are perpetrators. But most of them are just victims that have been hauled into hostile activities online and strategic conflicts by proxy. They have become first-hand targets of attacks and censorship rather than victims of collateral damage between conventional combatants as in the past.

The role of censorship in traditional warfare is small. It is different for cyber warfare in authoritarian regimes. For them, censorship is a defensive, and sometimes offensive, strategy to protect the domestic political order and make life difficult for dissidents, especially those who are alleged to be linked to foreign interests. Hence, it is not only a way to collect intelligence – it is a strategy to destroy the capacities of the perceived enemy. Furthermore, it is sometimes the only strategy at hand for a defence that will not wreck all other relations to foreign countries. Hence, in cases when authoritarian states believe they have a genuine threat at hand, they have to cast a very wide net with their censorship strategy. The affected sectors range from telecommunication and broadcasting networks to infrastructure and simpler conveyors of information. Even basic commercial services, such as online music, social networking sites and search engines could be (and have been) perceived as posing a threat to authoritarian regimes.

Thinkers supported by authoritarian states have introduced the concept of 'information sovereignty', suggesting that extends national sovereignty to encompass information and ideas passing across its borders.[45] Such arguments are not new. The idea of 'cultural imperialism' suggested that borderless flow of information was abused by large media outlets from the industrialised world, which justified a safeguard to protect the sovereignty of developing economies and to levee against external influence. The emergence of satellite communication and the Internet unsettled authoritarian governments who seek to disconnect their population from the rest of the world. If the target used to be Western popular culture from Disney and Hollywood it is now social media, search engines and cloud computing.

While the right to self-determination for all sovereign states without external interference is generally accepted as an indisputable axiom, information sovereignty has little to do with the right to self-determination as classically defined. Proponents of information sovereignty argue that control of the territory should extend to the flow of information across its borders, in the same way a sovereign state controls the exchange of goods across its borders. Stretching the statehood to minds of the people and exchange of ideas is basically a denial of freedom of thought. Rather than "sovereignty statehood", which stems from the consent of the people, it is instead a subordination of people under state authority in order to ensure survival of a political system.

The concept of information sovereignty is based on two erroneous assumptions. First, information sovereignty is assuming the purity of the indigenous thought; hence, no Iranian or Chinese would crave for the truth about what is actually happening in their countries, unless they were incited by external influence. Second, it assumed that foreign media is controlled by hostile powers or is an extended part of their powers. Such an assertion may hold true for a very few media outlets (such as Voice of America) but not for the vast majority of media enterprises, online and telecom services.

It is difficult for a government to devise an adequate response against balkanisation of the Internet, or to hostile actions against its businesses abroad. Unilateral withdrawal and sanctions are unworkable when such a broad range of firms as manufacturers of mobile phones, telecommunications networks, email services, business software and chemical plants are affected. It is impossible to declare all of them as 'strategic' or 'of vital national interest'

and prevent them from world trade, especially if a large economy like China is involved, as it would seriously damage the world economy. A favoured option by many security policy hawks and NGOs perhaps, but it simply is not a realistic option. So the responsibility to protect themselves against attacks is implicitly transferred back to the commercial actors. Producers of everyday goods like phones and software have to carry an unreasonable burden by being left to their own devices without any legal or physical protection, and by being forced to make moral and security-policy judgements that only can be done by states.

6. COMMERCIAL DAMAGE OF CENSORSHIP

Online protectionism

The Internet is today world's largest market place – and online retailing of physical and digital goods has made the www-address as real and valuable as any commercial real estate. Even authoritarian countries have a vibrant online economy. The turnover of Chinese online services has grown more than 60% year-to-year in the last three years. Market turnover from online advertising (which finances the lion's share of online services) is close to 25.6 bn RMB (□ 2.8bn).[46] China is not only spending time but also money online – the total turnover of e-commerce (including online retail), in China tops 260bn RMB (□ 28 bn) and is growing by more than 100% per year.[47] While it is true that China is far from the only country enforcing censorship, it may be the only country that enforces censorship for economic reasons.

Websites owned by foreign entities are facing discrimination regardless of whether they access the market from abroad through the firewall or operate as foreign-owned affiliates inside China. Arbitrary blocks target them disproportionately more often than their domestic competitors. It has been reported several times that traffic to some foreign sites has been redirected to the Chinese competitor or are blocked outright. Even if websites do not experience such drastic measures the access speed to the websites can be slowed down, rendering them useless. But, perhaps more importantly, censorship on the basis of moral standards is frequently applied to foreign-owned websites while domestic counterparts are left undisturbed. On several occasions, Yahoo, Google and Microsoft Bing were subject to crackdowns over pornographic materials while Baidu and other Chinese websites could produce exactly the same search results without getting blocked or censored by the government.[48]

In this environment, with privileged protection by the government against foreign competitors, local Internet services have flourished at the expense of others. Baidu, for instance, is by far the largest search engine in China today, which it was not just a few years ago. Baidu is also eyeing expansion abroad, and it follows a trajectory that resembles the mythology of some of the infant industry policies in the Asian Tigers: first develop under protection at home, then foreign expansion. YouTube and Facebook equivalents like Youku, Ren Ren Wang and Kai Xin Wang have replaced these original social networking sites, which have regularly been blocked. China's largest Internet portal Sina launched a near-identical micro-blogging service two months before access to Twitter was cut off.[49] As a consequence of the worsening business climate for online services, two of the largest Internet companies in the world, namely Yahoo and Google, have decided to effectively leave China, or radically cut down their presence to avoid exposing its business or clients to erratic censorship and surveillance. When they departed, their Chinese competitors got even more privileged positions on the Chinese market; on the same day Google announced it was considering leaving China, Baidu's stock on NASDAQ took a 16.6 % jump.[50]

In short, the Chinese government engineers a system of censorship that has the effect of boosting domestic operators at the expense of foreign businesses and it is the only country that legally and technically distinguishes the origin of the service provider and discriminates against foreigners. China has a clear mercantilist agenda to protect its domestic ICT sector and online content providers in particular. Therefore, it should not come as a surprise that on each occasion of crackdowns against foreign social networking sites, videos or search engines, domestic competitors have been relatively unharmed and their share prices have gone up.[51] China uses censorship to restrict foreign competition at home, and to give unfair advantages to local businesses. The censorship effectively fences the Internet off for government-approved actors that are politically reliable in the eyes of Beijing. But the commercial implications of digital authoritarianism do not stop at obstructing market access for web services. The forebodings about censorship spreading to other areas of technology have proven to be justified. An entire new range of services, for example software sales through mobile networks (so called apps), e-books, and licenses for cheap Internet calls via VoIP (such as Skype, MSN messenger and Google Talk) are restricted and eavesdropped. As wireless Internet (and so email and web browsing with it) has become a standard feature on phones, TVs and mp3 players etc., censorship has disseminated into other platforms than PCs and web browsing. This, in turn, has provoked Chinese custom authorities to establish restrictions on foreign import of such goods, unless they are open for tapping by the authorities, and restricted access for foreign-owned firms services such as geo-mapping that require them to fully function as devices or services.[52]

This development occurs in a policy climate where an increasingly self-assertive China is gradually decoupling itself from the market power of Western consumers. Domestic industrial policy ambitions have become more important than opening up markets. As part of that trend, China is asserting control over mobile and fixed line telecommunication services, encouraging consolidation between state-owned or controlled enterprises to enhance its control over the market. Overall, China and others are increasingly using discrimination against foreign business that in the end balkanises the ICT market. This fragmentation breaks up open networks and the ability to integrate markets for other reasons than national security concerns, but it also damages China's ability to increase growth and welfare. China has benefitted remarkably from trade in ICT goods, but is increasingly losing its position as labour costs increase. However, it performs very badly in transforming the technology sector into a more advanced service economy and has little capacity to climb the value-added chain. As a result, China's export of ICT services is about one-tenth of India's.

6. THE LOGIC OF A TRADE DISPUTE

Human rights, geopolitics and commerce hanging together

Previous sections in this paper have discussed the damaging effects of online censorship on human rights, cyber security and freedom of commerce. However, these three areas are not separated compartments with few or no connections to each other. On the contrary, they hang together: deteriorations in net freedoms typically affect them all. An intrusion on commercial freedom on the Internet, such as the blockage of websites, affects the commercial viability of online services, freedom of expression, and undermines the type of spontaneous-order infrastructure that gives the Internet its unique character and helps to make countries less vulnerable to cyber attacks. Similarly, actions to curtail online freedom of expression affect commercial freedoms and the security with which people can use online communications without fear of being under surveillance or putting themselves at risk.

From a policy perspective there are two important reasons to underline the integrated nature of these three concerns. First, there has been a tendency on the part of some to create a conflict between, for example, human rights and commercial freedoms online, or between cyber security and human rights concerns. Such conflicts may arise, but they are likely to be marginal in comparison with the commonality of the problems faced by these three legitimate concerns and objectives. Second, an improvement in one of these areas is likely to have positive effects on the other two. Most obviously, an end to blockages of commercial websites, for instance, will have a positive effect on the freedom of expression.

The real challenge that rather should occupy the considerations of policymakers and campaigners in the democratic world is: how can improvements be made? This is a genuinely difficult problem – and it is not about to go away. On the contrary, the problem will continue to grow as the Internet and online communications increase their role in the management of societies, businesses and everyday lives. Similarly, as countries like China grow to represent a big share of Internet traffic and online services, their view on how the Internet should be regulated will become more important for all countries. In a policy context the problem could be defined in this way.

1. The Internet and online communication thrive on freedom and open access. Geographical borders have from that viewpoint little if any relevance. It is a paramount aim to maintain this character of the Internet.
2. Improving access to the Internet and online communications in developing countries is of strategic developmental importance. This holds true also for countries with authoritarian or repressive regimes. It increases the ability of people to build greater connections to the outside world and it fosters in the long run the chances for political pluralism to take root in society. As a consequence, it increases the chance of geopolitical stability and peace. Bans, blockades or other instruments of protectionism will have the opposite effect.
3. Many authoritarian regimes have grown to become significant markets in their own right. China is the most obvious example. For most companies it is not an option to neglect the Chinese market. Nor can it be a guiding principle for other countries to deter its companies from engaging with countries like China. Not only does it flaunt the long-term ambition of integrating such a country into the world community, it is also economically damaging.
4. The infrastructure for maintaining civil freedoms and security online is somewhat different than in the physical world. To a larger degree it is embodied by private economic assets. Preventing the ability to get a good return on such assets, by curtailing its economic rights in countries like China, will first and foremost damage that particular asset, not the country in which it operates. Chinese authorities, for example, would welcome moves from other countries to prevent their companies from operating online services, or placing equipment for online communications, on its market.
5. Not responding to the problems posed by the restrictions of online freedoms, however, will make the problems grow bigger from all points of views. Censorship will proliferate and become an accepted norm, possibly even in democratic societies. The damages to sales will increase. And the vegetation for development of censorship technologies will become richer, threatening the ability of operators and authorities in democratic societies to keep track of developments.

Put differently, there are very few carrots and sticks other countries can use to get a country like China to change its practices. Moral suasion looks rather to be the only (in the short term as well as the long term) option that countries could resort to. And that will not take us far in addressing the problems that exist now. It would be wrong to say that traditional diplomacy has failed. Few countries have set themselves the ambition of changing censorship practices in a country like China with traditional diplomacy. It is important to increase diplomatic efforts, but no one should expect it to yield results if it operates alone.

One possible strategy that does exist, however, is to get countries like China to honour agreements it has signed. There are not many agreements around with a potential effect on online censorship. And the number of them gets even smaller if we also want them to be enforceable by legal means. We are practically only down to one: the General Agreement on Trade in Services (GATS) in the World Trade Organisation (WTO).

There are plenty of reasons to increase pressures on China for flaunting its WTO obligations in its current censorship. As will be argued later in this paper, China, and possibly also other countries, is in violation of its GATS commitments *when it uses censorship as a tool of discrimination* and *when its censorship actions are disproportionate to the stated aim of the actions*. Hence, the economic rights of other countries get violated by actions to censor the Internet and online communications.

Naturally, it is not all censorship actions that violate the rights of other countries; hence, a WTO case is not a strategy to address all problems caused by censorship. But important parts of censorship do violate economic rights. And as has been shown in past WTO cases of principal interest, it is possible to get a country like China to behave in better ways when countries defend their economic rights.

Dispute settlement under the WTO

The WTO is different from most other inter-governmental organisations. It has a body for dispute settlement that can intervene in the sovereignty of other countries to design its own policy. If a country has signed an agreement, it has to abide by the rules if it wants to avoid punishment. Sanctions are typically much more costly to the offending country than the action that breached WTO law in the first place.

Since the inception of the WTO Dispute-Settlement Body (DSB), countries have followed, reluctantly but voluntarily, the opinions of the DSB. Since China joined the WTO in 2001 it has (like most other big economies such as Europe and the United States) been found to violate WTO laws on several occasions and accepted the DSB's rulings. Past rulings have already effectively limited Chinese censorship by addressing the arcane ways in which China organises its media sector.

It should not come as a surprise that China has followed WTO rulings. China is a great beneficiary of WTO rules, which gives competitive Chinese firms protection against hostile moves by other countries to protect their domestic firms. Consequently, China is in favour of the WTO agreeing on even stronger rules, especially but not exclusively on contingency measures like trade remedies (e.g. anti-dumping). In fact, China is probably the WTO member with the strongest interest in protecting the integrity of WTO rules and rulings of the DSB.

Furthermore, trade policy in China is subject to the same forces as trade policy in other coun-

tries: companies and sectors competing to get favours from the state, inter-departmental fights, and lack of clear leadership from the top echelons of government. Until a few years ago, the departments working on trade reforms clearly had the upper hand and played it remarkably well. Up to the accession to the WTO, China undertook an unprecedented economic reform programme. The programme for economic modernisation continued after WTO accession, but was gradually watered down.[53] The Ministry of Commerce (Mofcom) in China is usually of the same opinion as most other commerce or trade ministries in the world: trade liberalisation is good, and protectionism is bad. Hence, it is not this ministry or other economic reformers that are responsible for the shift in China's commercial policy to industrial policy activism that discriminate against foreign firms. Often it has opposed such measures internally, but others have won the debate, frequently after getting support from the top brass of the Chinese leadership that has thwarted the reform programme. A WTO ruling against China, or any other move that signals legitimate concern on the part of other governments, may be seen as hostile by other departments, but typically not by Mofcom. As in other countries, such manifestations can help reformers to argue their case. If it goes as far as a WTO ruling, the force of the argument grows even stronger. Not even the economically illiterate camp of the Chinese leadership is willing to disregard such a rebuke of its policy.

Now, why is this crude history of China's trade policy in the 21st century of relevance? It gives an alternative view to the voices claiming China would never accept a WTO ruling that constrains its discretionary use of censorship. For instance, Daniel Drezner, a professor of international politics at Tufts University, writes on his Foreign Policy Magazine blog: "[...] if China were to lose such a case, one option would be to simply refuse to comply. The U.S. would be allowed to respond with trade sanctions, but I suspect China's government will take that bargain every day of the week and twice on Sundays."[54]

Such an outcome is a possibility. But this would carry a potentially expensive risk; China would not only be retaliated against by one country at one point in time. Other countries would be likely to join a WTO litigation case. If an offending country continued to flaunt its WTO obligations, it would have to continue to pay for it, ultimately until it withdrew from a WTO commitment (which is very expensive). But why do most observers assume China would not change policies found to violate WTO agreements? It is quite obvious that WTO litigation could not attack all online censorship in China. A case would target those measures that clearly are discriminating, disproportionate and plainly damage foreign firms. Furthermore, China has in fact already accepted a ruling of the WTO's highest legal body concerning its state monopoly and therefore de facto censorship on imported publications, music and films.[55] Importantly, that ruling established that China's monopoly was disproportionately harsh in relation to the objective of protecting public moral and security. And China accepted the ruling.

The legal grounds for a WTO case

A DISPUTE AT the WTO will concern the commercial aspects of online censorship. This is not to say that other pressing aspects – such as the conditions for human rights and cyber security – would not be positively affected by a ruling against a country like China. But the litigation itself would only have to concern alleged violations of commitments made to other countries in the WTO. This is not a bad starting point for efforts to combat the current spread and undisciplined use of online censorship. It singles out the commercial aspects (and market access aspects in particular) and addresses problems in a fairly apolitical forum. The case cannot be argued on moral grounds; such arguments would be thrown out immediately. At

the centre would rather be the unrelentingly dry logic of law and jurisprudence. However, the limit of the WTO approach is that litigation would have to be confined to market access commitments by countries that are members of the WTO. That leaves many of the worst offenders beyond reach – Iran and North Korea, for example. But there is one country that cannot claim this status: China.

In a previous study, we have argued that most types of online services would fall under China's commitments for market access from abroad, or through an affiliate inside China.[57] This is the central part of any potential litigation of China's online censorship because it commits the country to non-discriminatory treatment of foreign enterprises for those services. Furthermore, the paper argued that WTO jurisprudence rests on concepts like technological neutrality that provides equal protection for the new digital services as for their offline counterparts. Nor do we put much weight on the counter-argument that many online services, like a search engine, did not exist at the time the GATS was signed in 1994, and that a country therefore cannot be obliged to keep markets open in those services. The Appellate Body undermined that argument in its ruling against the United States on online gambling. Furthermore, when China joined the GATS in 2001 services like search engines and blogs actually did exist. Yet China decided not to make any special exemptions for them, although it was free to do so. China is clearly bound by GATS disciplines through its admission of non-restricted access to online processing services. Neither is China alone to make such commitments: Interesting to note here is how Saudi Arabia, UAE, Oman, Jordan have all made similar commitments.[58]

Several measures that China employs in its discriminatory censorship – like deliberately slowing down access to overseas sites, rendering them useless, or simple arbitrary blocks (especially if they occur without proper notification) – are likely inconsistent with GATS rules. China will most certainly fail to prove that foreign online services do not face discriminatory treatment compared to domestic providers who do not face any sanctions for identical services. The regime of ICP-licences is likely to be regarded as an unauthorised de facto nullification of the market access commitments that China has made and is bound by.

As a final caveat, WTO case law acknowledges the discretionary right of its members to make exemption on the grounds of defence for public moral and order. It even acknowledges the sovereignty of its members to set a standard for public morals. However, there are strict conditions for such exemptions, and China failed on those conditions when it tried to defend censorship in the case of audio-visual imports. It is not likely to be successful this time either. First, China must prove that the arbitrary blocking of websites is an absolute necessity to obtain the level of morals it pursues. It is unlikely that China, or any other censoring country, will be able to get that free pass. Second, China must prove that there are no reasonably available alternative measures that are less trade restrictive. In this case, the bare existence of selected filtering through the Great Firewall of China, and its regulatory system of self-discipline, prove that there are fewer trade restricting measures available than outright blockage of websites on protectionist grounds. Admittedly, this argument presupposes that selective filtering of individual pages, sensitive key words, and self-discipline rules would be considered to be in accordance with WTO law. But even if filtering, too, is a menace, it is unlikely that the WTO would rule against such use, provided it is not done in a fashion that clearly discriminates against foreign providers of online services.

7. CONCLUSION

The government of China has been remarkably successful at adapting to the perceived dangers posed to their political authority by the Internet. While it promotes its usage to benefit economic growth and industrial development, the Chinese Communist Party has also turned the Internet into a tool to control and maintain political stability. President Hu Jintao even proclaimed: "Whether or not we can actively use and effectively manage the Internet...will affect national cultural information security and the long-term stability of the state".[57] This is reflected in the increase in Internet-related arrests. An increased use of cyber espionage and military development has helped to further China's foreign policy goals and increased geopolitical leverage abroad.

In hindsight, the early hopes that the Internet would quickly usher in a wave of new pluralist political reforms in authoritarian countries like China now appear naïve. It has yet to happen. It may, however, happen in future, and it is incorrect to assert, as some do, that the Internet will never be a catalyst in reforming the Chinese political system. But for the moment digital authoritarianism has the upper hand over digital liberation, to put it in more dramatic and Manichean terms. The view this paper purports is that foreign actors can help to redress this imbalance by taking China to the WTO for flaunting its commitments in the GATS.

Principally, a WTO case against online censorship could not attack the entire system of censorship in China or any other country. To be successful, WTO litigation will have to target the aspects of censorship that are discriminatory and disproportionate. But that is a good starting point for a more structured response by other countries to the proliferation of online censorship.

Firstly, it would demonstrate that there are boundaries in international law to what governments can do and limit the discretion with which China runs its system of online censorship. This is a big step forward and it is very likely to decrease the extent of online oppression.

Secondly, it would force countries to take full control and responsibility over the execution of their censorship policy. There are today too many examples of authorities, or freelancers operating with semi-authority, that act discretionally, sometimes with little or no support in domestic law. Greater state control over censoring authorities is a prerequisite to limiting the damages of online censorship. Hence, the rule of law should also be applied in authoritarian regimes.

Thirdly, it would give online service companies – today in the line of fire – greater protection from arbitrary actions that severely damage their business and offer an alternative to voices calling for unilateral trade measures to be erected against perpetrating countries and countries involved in trade in those countries.

BIBLIOGRAPHY

China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products, World Trade Organization, DS 363

China – Measures Affecting Financial Information Services and Foreign Financial Information Suppliers, World Trade Organization, DS 372

Erixon, Fredrik, Messerlin, Patrick, Sally, Razeen & Wang, Jinghui, *'China's Trade Policy Post-WTO Accession'* in *'The Future of Asian Trade and Growth'*, Routledge, 2010

Hindley, Brian, Lee-Makiyama, Hosuk, *'Protectionism Online: Internet Censorship and International Trade Law'*. ECIPE Working Paper, No. 12/2009

Human Rights Watch, World Report 2010

Information Office of the State Council, *'The Internet in China'*, June 2010

Landes, David, *'The Wealth and Poverty of Nations'*, W.W. Norton, 1998

OpenNet Initiative, http://www.opennet.org

Pei, Minxin, *'China's Trapped Transition: The Limits of Developmental Autocracy'*, Harvard University Press, 2006

Reporters Without Borders, Index of Press Freedom, 2010

Zakaria, Fareed, *'The Post-American World'*, W.W. Norton, 2009

ENDNOTES

1. China Internet Network Information Center, '2*6th Statistical Survey Report on Internet Development in China*', 2010, http://www.cnnic.cn/uploadfiles/pdf/2010/8/24/93145.pdf
2. Hindley, Brian, Lee-Makiyama, Hosuk, 'P*rotectionism Online: Internet Censorship and International Trade Law*'. ECIPE Working Paper, No. 12/2009
3. Commissioner Neelie Kroes quoted by Willis, A, '*EU hits out at Chinese Internet censorship on trade grounds*', EU Observer, May 18, 2010
4. Bangkok Post, March 8, 2010, '*Man arrested for lese majesty SMSs*'
5. Cropley, E, '*BBC rejects Thai royal slur complaint*', Reuters, June 2, 2008
6. *LICRA vs. Yahoo Inc et Yahoo France*, 2000/05/22
7. OpenNet Initiative, http://www.opennet.org, 2010
8. See note 2
9. Hille, K, '*Internet restored to restive Xinjiang region*', Financial Times, May 14, 2010
10. Zittrain, J. & Edelman, B., '*Empirical Analysis of Internet Filtering in China*', Berkman Center for Internet & Society, Harvard Law School, 2003
11. Greenley, Brendan, Drajem, Mark, '*China's Facebook Syndrome*', Business Week, March 14, 2011
12. Pei, Minxin, '*China's Trapped Transition: The Limits of Developmental Autocracy*', Harvard University Press, 2006; Zakaria, Fareed, '*The Post-American World*', W.W. Norton, 2009
13. Landes, David, '*The Wealth and Poverty of Nations*', W.W. Norton, 1998
14. Chinese Internet Network Information Center, 2007

15. Esarey, Ashely, Qiang, Xiao, '*Political Expression in the Chinese Blogosphere: Below the Radar'*, Asian Survey, September/October, 2008, Vol. 48:5

16. Information Office of the State Council, '*The Internet in China*', June 2010

17. Jacobs, A, 'Chinese Government Responds to Call for Protests', New York Times, February 20, 2011

18. China – Measures Affecting Financial Information Services and Foreign Financial Information Suppliers, DS372

19. Xiao, Q, '*Latest News from the Ministry of Truth: May 11-12, 2010*', China Digital Times, http://chinadigitaltimes.net/2010/05/latest-directives-from-the-ministry-of-truth-may-11-may-12-2010/, May 13, 2010

20. Human Rights Watch, World Report 2010

21. Reporters Without Borders, http://en.rsf.org/Internet-enemie-china,36677.html, 2010

22. '*Surveying Internet Usage and Its Impact in Seven Chinese Cities*', Centre for Social Development Chinese Academy of Social Sciences, November 2007

23. Clinton, Hillary, '*Remarks on Internet Freedom*', January 21, 2010

24. Bildt, Carl, '*Tear down these walls against Internet freedom*', Washington Post, January 25, 2010

25. US Congress, H.R. 275, January 5, 2007

26. Hillary Clinton interviewed by Bloomberg TV, http://www.state.gov/secretary/rm/2010/03/138677.htm, March 19, 2010

27. European Commission, High Representative of the Union for Foreign Affairs and Security Policy '*A Partnership for Democracy and Shared Prosperity with the Southern Mediterranean*', COM(2011) 200

28. '*Cryptography, Iran and America: Worse than useless – An American government attempt to help Iranian dissidents backfires*', The Economist, September 16, 2010

29. NATO, Lisbon Summit Declaration 20 November 2010

30. Mann, J, '*Panetta Warns Cyber Attack Could Be Next Pearl Harbor', The New New Internet*, http://www.thenewnewInternet.com/2010/04/21/panetta-warns-cyber-attack-could-be-next-pearl-harbor/, April 21, 2010

31. 'Intel Chief: US At Risk From Crippling Cyber Attack', FoxNews, http://www.foxnews.com/politics/2010/02/03/intel-chief-risk-crippling-cyber-attack/, February 3, 2010

32. McCullagh, Declas, '*Obama on Cybersecurity: We're not that Prepared*', CNET News, http://news.cnet.com/8301-13578_3-10252154-38.html?tag=mncol;txt, May 29, 2009

33. CSIS Commission on Cybersecurity, '*Securing Cyberspace for the 44th Presidency*' Washington, DC, 2008

34. The Bipartisan Policy Centre, '*Cyber ShockWave*', February 2010

35. Ibid

36. Council of the European Union, '*A Secure Europe in a Better World – European Security Strategy*', December 12, 2003.

37. Council of the European Union, '*Report on the Implementation of the European Security Strategy – Proving Security in a Changing World*', December 11, 2008

38. 'Merkel China Visit Marred By Hacking Allegations', Der Spiegel, http://www.spiegel.de/international/world/0,1518,502169,00.html, August 27, 2007

39. Gartzke, U, '*Outrage in Berlin over Chinese Cyber Attacks*', The Weekly Standard, http://www.weeklystandard.com/weblogs/TWSFP/2007/08/outrage_in_berlin_over_chinese.asp, August 31, 2007

40. Hersh, Seymour M, 'The Online Threat', The New Yorker, November 1, 2010

41. England, Andrew, 'UAE lifts BlackBerry ban threat', Financial Times, October 8, 2010

42. Drummond, David, '*A New Approach to China*', Official Google Blog, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html, January 12, 2010

43. Forthcoming paper by Lee-Makiyama, H
44. Kirschgaessner, Stephanie, 'Huawei U-turn on US deal saves blushes', Financial Times, February 20, 2011
45. See Mowlana, Hamid, '*Global Information and World Communication: New Frontiers in International Relations'*, 1997; Gong, W, 'Information Sovereignty Reviewed', 2005
46. Data Centre on the Chinese Internet, http://www.dcci.com.cn/dynamic/view/cid/3/id/394.html, 2011
47. '*China sees online sales booming in 2009*', People's Daily, December 2, 2009
48. Calinoff, J, '*Where Google Loses*', Foreign Policy, September 2009; 'NSFW Google, Not Baidu, *Getting Punished for China Porn Searches*', Venture Beat, http://venturebeat.com/2009/06/19/nsfw-google-not-baidu-getting-punished-for-china-porn-searches/, June 19, 2009
49. Calinoff, J, '*Beijing's Foreign Internet Purge', Foreign Policy*, January 2010
50. Ibid.
51. Ibid.
52. '*China cracks down on illegal online map services to protect state security*', People's Daily, March 26, 2008
53. Erixon, Fredrik, Messerlin, Patrick, Sally, Razeen & Wang, Jinghui, '*China's Trade Policy Post-WTO Accession*' in '*The Future of Asian Trade and Growth*', Routledge, 2010
54. Drezner, Daniel, '*A Technical Solution to a Political Problem?*' Foreign Policy Blog, http://drezner.foreignpolicy.com/posts/2010/02/04/a_technical_solution_to_a_political_problem, February 4, 2010
55. China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products, DS 363
56. Lee-Makiyama, Hosuk, 'Google and Goliath: How free trade and WTO unknowingly pioneered free speech', The Majalla, http://www.majalla.com/en/economics/article55885.ece, May 20, 2010
57. This paper only summarizes the arguments of that paper briefly. To get the full technical flavour of our analysis, please see Hindley, Brian & Lee-Makiyama, Hosuk, 2009, *Online Protectionism: Internet Censorship and International Trade Law*. ECIPE Working Paper, No. 12/2009
58. Dickie, M, '*Hu Seeks to Purify Internet*', Financial Times, January 25, 2007