An inter-*nation*-al Internet:

China's contribution to global Internet governance?

David Kurt Herold
Department of Applied Social Sciences,
Hong Kong Polytechnic University,
Email: ssherold@inet.polyu.edu.hk

Abstract:

The first decade of the 21st century saw the Internet grow exponentially, and enter 'mainstream' culture, which brought the increased attention of the 'general public', the media, and government authorities. This meant a growth of awareness for the 'dark side' of the Internet, e.g. its use in the pursuit of criminal, or socially unacceptable activities, and a resultant drive by governments to create legal frameworks to tame the wilderness of Cyberspace.

Legislatives, and judiciaries of various countries have acted to curb online excesses, and in the process they have begun to shape the future of the Internet as a whole. Authorities in the United States decided to ban online gambling and issued warrants for the arrest of non-US citizens, not resident in the USA French court forced Yahoo to stop displaying Nazi memorabilia on auction sites accessible in France. UK laws require organisations to monitor all electronic communication on computers used on their premises. China forced Microsoft, Google, and Yahoo to obey Chinese regulations regarding 'sensitive information', etc. The global Internet has increasingly become a fiction, amid national regulations for the Internet, the citizens of a particular state may access.

Most of these developments have been ad-hoc, and largely uncoordinated responses to specific situations and problems. However, the overall effect of these steps has been to change the Internet in ways largely ignored both by the general public. A White Paper on the Internet, published in June 2010 by the Chinese government, offers a perspective on the consequences of these changes in their totality, though, as it outlines the official Chinese stance on the future of the Internet and on the role of national governments in the governance of online spaces, which appears to gather the different national efforts to regulate the Internet into one cohesive system.

The Chinese government's White Paper argues that the Internet has become a central, and essential part of a country's socio-economic system, and that therefore the governments of individual countries should be empowered to both safeguard, and control it, in the interest of their national well-being. Once each country's Internet has come under the purview of its government, the global networking of the separate national Internets should be regulated through the application of existing and continuously evolving treaties between nation states, similar to all other national concerns. Instead of a global, unregulated Cyberspace, a regulated, and diverse Internet of Nations would result, in which different countries could promote their own cultures according to their own legal needs and wishes, under the aegis of the United Nations, and not the U.S. controlled ICANN.

This presentation will argue that despite U.S. protests against the White Paper, it represents the logical endpoint of previous efforts by governments of different countries, including European and American ones, to regulate and control the Internet. The seductiveness of the Chinese proposals to the governments of nation states, both in the developed, and in the developing world, as well as the increasing status of China on the world stage suggest that the idea of an Internet of Nations should be taken seriously, and should be addressed and scrutinized by Internet scholars and the general public.

An inter-*nation*-al Internet:
China's contribution to global Internet governance?

David Kurt Herold, Hong Kong Polytechnic University

Over the course of the past two decades the Internet in its many, and ever-changing incarnations has become almost as commonplace and ubiquitous as telephones. People visit sites and pages on the world-wide-web, chat on their computers with friends, family, and colleagues, employ 'apps' that obtain information online, store data on webservers, etc. The massively increased use of such networking technologies has resulted in the development of ever easier networking 'tools', as well as a growth of 'objectionable' uses of the Internet.

The Internet has become easier to use, as users do not have to worry about any of the networking framework or the underlying technologies to access it. Pointing and clicking, coupled with a few, very basic skills, e.g. typing, choosing the right software, etc. allow almost anybody to start a video chat with another person in another country, and to transmit files to them. The end-user doesn't have to worry about the TCP/IP protocols, location of ISP servers, the routing of messages, choices of backbone server connections, datastream conversions, network packages, etc. – it is all handled for them, including the 'crossing' of national boundaries and jurisdictions.

The easy crossing or avoiding of national boundaries using networking technologies has led to a rise in complaints about some of the data available online. From the clear-cut case of 'child pornography' to cultural and legal differences in attitudes towards gambling, religious jokes, language choices, etc. the use of the Internet has raised important questions about the sovereignty of nation states and the limits of the jurisdiction of national governments. A simple (simplistic?) example can serve to illustrate the issues at stake here:

User X from China and user Z from Germany meet in the 3D online world 'Second Life'. After some initial chit-chat, X complains about Z's choice in avatar and asks 'Why would anyone want to look like a nigger?'

In China, such a question would pass without comment. In Germany, racism is illegal, and Z would probably feel offended, while in the USA, where the servers for Second Life are located, the choice of the word 'nigger' would cause additional problems. How to judge this

situation, then? Whose values to apply? Does it matter that English is neither X nor Z's mother tongue? Are the two people 'meeting' online, and if so 'where'? Is this an example of 'communication' between a Chinese person and a German person using available technologies? Should 'the Internet' be treated as similar to the telephone, i.e. a communication technology, or as something different?

Manuel Castells (2010 [1996]) and others have argued that the Internet represents the emergence of a new kind of society or a fundamental change of existing societies, emphasising its 'networking' effects, and its value as part of 'Information and Communication Technologies' (e.g. Dutton & Jeffreys, 2010), thus placing the emphasis on the *offline* users who are connected to each other through technology, and the changes this technology is causing *offline*. While this approach to the Internet has proved to be very fruitful, and provided the basis for many valuable studies of societal developments over the past twenty years, this paper wants to suggest that such approaches are failing to take into account developments in the non-academic world, in which state actors are shaping a future for the Internet that follows a very different logic, and that could radically transform the Internet from being a *global Information Network* into a collection of *inter-connected national Intranets*.

The paper will first employ a number of examples from the past decade to illustrate the creeping nationalisation of the Internet, i.e. the splintering of the global Internet into different, locally-accessible versions of the Internet. This will be followed by an analysis of a White Paper on the Internet published by the government of the People's Republic of China in June 2010, which is to date the clearest expression by a state actor on their desired future development of the Internet as a regulated network of state-controlled, national Intranets. The Chinese state's suggestions will then be placed into a more general framework through a comparison with the emergence of the concept of the 'nation-state', and an overview over some of the statements made about the Internet by state actors in 2011. This paper wants to propose that it might be advisable for academic discussions of the Internet to adopt 'spatial' metaphors for the Internet, if they want to influence political debates about the future of the Internet, if they wish to influence the transformation of the global Internet into an inter-*nation*-al Internet.

The creeping nationalisation of the Internet

In 2000, a French judge ordered Yahoo, the US Internet giant, to make it impossible for French Internet users to bid for Nazi memorabilia from World War II on their auction site, as such memorabilia are illegal in France (Enos, 2000). Yahoo decided to fight this decision in the interest of keeping the Internet free from government interference, and a year later a judge in the USA 'overturned' the ruling of the French courts. The US judge argued that Yahoo did not have to follow the ruling of the French courts, as Yahoo as a US firm had a constitutionally guaranteed right to '*freedom of expression*' (Lawson, 2001) which they were exercising when posting materials online. The French state appealed this ruling, though, and three years later the French verdict was upheld on appeal. The 9th US Circuit Court of Appeals argued that a US court could not interfere with or set aside the rulings of a foreign court that the USA recognised (Pinsent Masons, 2004). As a result, Yahoo would have to censor those parts of their website accessible from inside France, i.e. localise their auction site. For the Internet in general, this was an important decision, as it meant that the French interpretation of the Internet as being data or media services accessible to end-users living in a specific jurisdiction was affirmed as 'valid' for all Internet pages accessible by end-users living in France, thus creating a 'local' version of the 'global' Internet.

In a case also involving the posting of information by users of a globally accessible website, three Google executives were convicted in Italy in 2010, after a user posted a video to YouTube that showed several Italian school children bullying a mentally disabled child (Ryan, 2010). The Google executives were condemned for not taking down the video 'fast enough', thus in effect requiring YouTube and its parent company Google to vet all videos accessible to Italian end-users before posting them online. Probably as a result of this judgment, Google was quick to shut down the blog of a critical Italian blogger after receiving a court order to do so, although the order came from the prosecutor who was being criticised on the blog, and apparently aimed at silencing this critical voice (Cartier, 2011). American notions of 'freedom of speech', or of 'online freedom' became subject to Italy's laws, and 'the Internet' had to be localised for Italian end-users.

In a far more forceful demonstration of the state's power to enforce local regulations online, US law enforcement officials arrested numerous people in 2006 (McCarthy, 2006) and in 2008 (Kearney, 2008) for running websites offering sports betting to citizens of the USA.

Neither the owners of the websites, nor the servers running the sites were located in the USA, but the American authorities argued that the sites were illegal in the USA, accessed by US citizens, and therefore the owners of the sites were liable under US law. British nationals were extradited to the US on the charge that they should have collected US taxes from all US bettors, even if the sites were 'off-shore' (Kennedy & Doran, 2006), and the European Union was pressured into agreeing with the prosecution of Europeans and European betting sites, despite previous agreements to the contrary (Kearney, 2008). Again, a state actor had decided that the location and nationality of the end-users of the Internet was the place of jurisdiction, and other governments had concurred, thus forcing another part of the Internet to introduce end-user location-scanning, and the offering of localised versions of the Internet to its users.

The effect these and other, similar cases have had on the Internet as a whole is measurable in the degree to which the Internet has become localised during the past decade. Google's offerings, from Search results to Google News to GMail or even Google Scholar, have all received location-aware makeovers that offer end-users different results and a different interface based on their IP address. Other 'global' Internet companies, e.g. Amazon, Ebay, Facebook, Yahoo, etc. have followed suit and localised their Internet offerings, while making it difficult to access services from other localities. While this has led to easier access to Internet services by users not proficient in other languages, the 'splintering' of the Internet has reinforced notions of nation states control and responsibility over and for the Internet accessible to their citizens.

The 2010 Chinese Whitepaper on the Internet

In China the government has been more active in its engagement with the Internet than in most other countries. From the start, the Chinese Internet was set up very differently to the Internet elsewhere. During the 1990s, the central government of China set up four state-owned entities to provide Internet access in China, and even after the provision of private Internet access in 1997, this arrangement persisted. The Chinese state kept ownership and control over the access routes to the Internet, and only allows private enterprises and individuals to rent bandwidth from state-owned enterprises.

The Chinese state or state-controlled entities own the physical backbone of the Internet in China, which is very different from other countries, where private Internet Service Providers

compete against each other under the jurisdiction of the state. This means, the Chinese government did not have to gain control over the Internet, or react to developments online, but has to explicitly or implicitly allow everything that happens in Chinese cyberspace. The Internet in China, run on state-owned hardware servers, state-owned fibre-optics, via state-owned switches is 'government allowed'.

> "China has injected enormous sums of money into Internet infrastructure construction. From 1997 to 2009 a total of 4.3 trillion yuan was invested in this regard, building a nationwide optical communication network with a total length of 8.267 million km."
>
> (Information Office of the State Council of the PRC, 2010)

This control of the Chinese government over the Internet in China has led to a quasi-separation from the rest of the world-wide Internet. The control exercised by the Chinese government over the Internet in China has created enough obstacles and hassles for Chinese Internet users to make 'international' Internet access slow and undesirable, though not impossible (Herold, 2011c). As Sherman So argued, "China is not on the Internet, it's basically an intranet" (as quoted in Fong, 2009; see also So & Westland, 2010). The lack of speed, occasional time-outs, and blocked sites make any access to non-Chinese websites from within China unattractive enough for Chinese Internet users not to bother trying (Roberts, 2011). As a result, Chinese cyberspace remains largely separated from the rest of the world, and has developed many unique features, including a much greater engagement of government officials with Internet users on forums, blogs, micro-blogs, etc. (see e.g. Bandurski, 2011; Chu & Cheng, 2011; Farrall & Herold, 2011; Herold, 2008, 2010, 2011b; Meng, 2011).

In June 2010, the State Council of the People's Republic of China published a White Paper on the Internet in China, outlining their vision for the future of not only the Chinese, but the global Internet. It defines the role of nation states and governments in relation to the Internet, and frames the debate not primarily in terms of 'information' or 'communication', but rather as a necessary outgrowth of the economic importance of the Internet, particularly in developing countries.

> "The Chinese government fully understands the Internet's irreplaceable role in accelerating the development of the national economy, pushing forward scientific and technological advancement, and expediting the informational transformation of social services, and places emphasis on and actively supports Internet development and application."

(Information Office of the State Council of the PRC, 2010)

Within this frame of reference, the supervision of the Internet by national governments is logical and unavoidable. Any facet of "the national economy" that plays an "irreplaceable role" has to be safeguarded against both external, as well as internal threats, and policed by the authorities to guard it against interference.

> "To build, utilize and administer the Internet well is an issue that concerns national economic prosperity and development, state security and social harmony, state sovereignty and dignity, and the basic interests of the people. The government has a basic policy regarding the Internet: active use, scientific development, law-based administration and ensured security. The Chinese government has from the outset abided by law-based administration of the Internet, and endeavoured to create a healthy and harmonious Internet environment, and build an Internet that is more reliable, useful and conducive to economic and social development."

(Ibid.)

The Internet regulations of the Chinese state are not meant as a straight-jacket to control the development of the Internet, or to prevent criticism of the government as such – although there is a high level of censorship on the Chinese Internet (Herold, 2011a; Mu, 2011; Xinhua News Agency, 2011). Regulations have frequently been adjusted, and will continue to be adjusted to meet new developments, and to allow for emerging needs. The Chinese government is particularly interested in not doing this in isolation, though, but in collaboration with other governments who – according to the Chinese understanding of the Internet – are in a similar position of needing to safeguard their citizens' access to the Internet to protect their national economies.

> "The Chinese government will constantly adjust relevant policies to better match the inherent law and the objective requirements of the development and administration of the Internet. While absorbing good experiences of other countries in developing and controlling the Internet, China is prepared to work with them for the further progress of the Internet."

(Information Office of the State Council of the PRC, 2010)

The importance of the Internet to China's national economy means that "Internet security is an important part of China's Internet administration, and an indispensable requirement for protecting state security and the public interest" (Ibid.). The Chinese government has therefore not only the right, but also the duty to ensure the smooth running of the Internet, as it is "an

important infrastructure facility for the nation" (Ibid.). These arguments, based in political-economy discourses lead to the logical conclusion that

> "within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The *Internet sovereignty of China* should be respected and protected. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security."
>
> (Ibid. - my emphasis)

This statement and claim by the central government of China is important, as it serves to redefine the Internet. The Internet and related technologies are not merely information and communication technologies (ICTs), but more than that. Its economic value to the national economy turns 'cyberspace' into *legal territory* under the jurisdiction of the nation state. Not only end-users of the Internet, or the parts of the Internet accessible to them, but *all* Internet data *on* servers located inside the territory of the People's Republic of China have to obey the laws of the PRC.

The *Internet sovereignty* the Chinese government claims for itself is a concise summary of the state ownership of and the many regulations for the Internet that limit Chinese cyberspace, and as such not very surprising. Through the connotations of the term 'sovereignty', though, the Chinese claim also proposes a new model for the *international* Internet that challenges the more idealistic constructs of a world-wide network in which users freely communicate and exchange information. While non-Chinese conceptualisations tend to focus on the individual users of the Internet, on their contributions, their rights, etc. in a global environment, the Chinese framework sees the individual user as part of a 'nation', i.e. as embedded in cultural traditions, economic structures, political sovereignties, etc. Although *individual* users might prefer a *globalising* approach to the Internet that allows them to interact freely with Internet users from around the world, the '*group of users*' living under the jurisdiction of a *specific state* has needs that supersede the naive (?) perspective of the individual.

> "National situations and cultural traditions differ among countries, and so concern about Internet security also differs. Concerns about Internet security of different countries should be fully respected. […] Though connected, the Internet of various countries belongs to different sovereignties."
>
> (Ibid.)

In Germany and France, Nazi memorabilia are illegal, in the USA gambling is restricted. Each nation state has its own legal, and cultural sensitivities that are expressed in national laws and regulations. The Chinese White Paper is arguing that these laws and regulations ought to apply to *all* 'areas' under the jurisdiction of the state, not only to the *offline* ones. Instead of the *ad-hoc* application of laws to problem-cases online, as in the examples provided earlier, the Chinese government argues for the pre-emptive legal clarification of the status of the Internet worldwide, i.e. for an integration of the Internet into the existing international political structures.

> "Though connected, the Internet of various countries belongs to different sovereignties, which makes it necessary to strengthen international exchanges and cooperation in this field. China maintains that all countries should, on the basis of equality and mutual benefit, actively conduct exchanges and cooperation in the Internet industry, jointly shoulder the responsibility of maintaining global Internet security, promote the healthy and orderly development of the industry, and share the opportunities and achievements brought about by this development."
>
> (Ibid.)

The zoning of the Internet into different national sovereignties would result in the emergence of *national Intranets* under the jurisdiction and control of national governments, whose *inter*-connection is governed by "bilateral dialogue and exchange mechanisms" (Ibid.). Similar to the movements of people and goods across international borders, the flow of data would be regulated as well, and the cooperation between different governments would become crucial.

> "In order to draw on the experience of other countries in developing and administering the Internet industry, the Chinese government has organized dozens of delegations since 2000 to pay visits to more than 40 countries in Asia, Europe, North America, South America and Africa, and has applied some of their successful experiences to its own Internet development and administration. "
>
> (Ibid.)

The current Internet system, grown out of its early beginnings in the USA under the loose administration of – from a Chinese perspective – the *US-American* Internet Corporation for Assigned Names and Numbers (ICANN) is unacceptable within this framework. For the Internet to develop fully, and for all countries to share fully in the advantages the Internet provides, the Internet can no longer be controlled by the citizens of only one country. Instead, *all* countries should share in the administration of the Internet based on international treaties.

> "China maintains that all countries have equal rights in participating in the administration of the fundamental international resources of the Internet, and a multilateral and transparent allocation system should be established on the basis of the current management mode, so as to allocate those resources in a rational way and to promote the balanced development of the global Internet industry. *All countries should conduct multi-form, multi-channel and multi-level exchanges and cooperation in this regard* on the basis of equality and mutual benefit."
>
> (Ibid. - my emphasis)

The Chinese vision of the Internet would effectively create a loosely connected system of national Intranets, whose gateways are controlled by national governments. An inter-*nation*-al Internet should be governed by national codes of law, existing international agreements, and (to be agreed) international Internet agreements. This should then be embedded within existing international frameworks for cooperation between nation states, and supervised by the *United Nations* as already established, legitimate, supra-national body for interactions between nation states.

> "China holds that the role of the UN should be given full scope in international Internet administration. China supports the establishment of an authoritative and just international Internet administration organization under the UN system through democratic procedures on a worldwide scale."
>
> (Ibid.)

The Chinese Whitepaper, in short, constructs the Internet as an extension of existing (offline) national space, under the jurisdiction of the specific government of a nation state. In this setting, the Internet is more than just a channel or communication, for the transmission of information, but is instead seen as *online space* – the term 'virtual' being counterproductive. The 'story' of the Internet of the past 20+ years is then re-cast as a repetition of the settling of the Wild West of the USA:

The Internet used to be a wild, unregulated, border-less place for pioneers and individualists. This began to change as Civilisation arrived to protect the weak and facilitate the exploitation of economic resources. Robber-barons of the Internet arose (e.g. Google) who are still wielding a lot of power (2011), but their era will soon end, as civilisation expands and the state gets ready to challenge their powers. The wilderness is settled and made habitable for all through infrastructure improvements and the elimination of dangers. 'Settled areas' are created (Facebook, Twitter, 'Apps') and 'the law' has arrived to watch over the now settled territories ready to join 'the Union' (offline world).

Imagining the Internet

In 1983, Benedict Anderson published a book on the development of the concept of 'nationalism' and the emergence of 'nation states' that continues to be highly influential (B. R. Anderson, 1991). While a full discussion of his theses is beyond the scope of this paper, his description of the nation state provides an interesting comparison to the Internet as conceived by the Chinese state. Anderson argues that the nation state emerged as a concept in the late 18th century out of the *shared imaginations* of communities of people living in specific, clearly delineated areas under the rule of one government, and sharing certain narratives about their past (1991, p. 7). The nation state was not, however, the invention of the people themselves, but rather "from the start a conscious, self-protective policy, intimately linked to the preservation of imperial-dynastic [= national] interests" (B. R. Anderson, 1991, p. 159).

During the emergence of nation-states, governments supported the creation of narratives that supported shared 'national myths' containing exemplars of 'national characteristics', e.g. 'punctuality', 'hard work', etc. in the Fairy Tales of the Brothers Grimm in Germany. In the context of the Internet, similar narratives support the increased involvement of the state in the administration of online spaces by e.g. pointing to the "development of the national economy", "people's increasing demands for information", and the creation of "e-government while enhancing the capability of governance" as the main features of the Chinese Internet, while deprecating its entertainment value or its suitability for criticising the government (Information Office of the State Council of the PRC, 2010).

New narratives are used to describe the Internet – even outside China – that suggest the involvement of the state as a logical step in the development of the Internet. The Internet is increasingly described as a dangerous place, full of "cyberspace sex offenders" (Fairfax Media, 2011), against whom Internet users should be on the constant look out (Peterson, 2011). Terrorists are using the Internet to recruit suicide bombers (Binoual, 2011), while scammers employ it to cheat more people than ever before (Conroe Police Department, 2011). Irresponsible and criminal Internet users are endangering companies (Marsden, 2011) and public safety (Jackson, 2011) through their unsupervised behaviour online, while theft (Forde, 2011) and destruction of property (Arthur, 2011) are widespread.

The state is needed to protect its citizens online. E-commerce and e-citizens have a right to a secure environment – provided and policed by the State. Security agencies and police forces increasingly get involved in ensuring the safety of e-citizens and their legitimate online pursuits (Kaiser, 2011; Vijayan, 2011). Slowly, but inevitably (?) the global Internet, once cast as the 'last free place on earth' where anonymous web surfers could meet and interact irrespective of their age, race, gender, religion, sexual orientation, etc. is turning into the online extension of existing offline nation states and their legislative strictures.

The desire of citizens to be protected online, and the demands by companies for the enforcement of laws in cyberspace combined with the goal of nation states to control *all* territories under their power have made the splintering of the global Internet into national zones of online spaces almost unavoidable. The enforcement of laws online is only possible if the nation state can prove that specific 'areas' of the Internet are under its jurisdiction, and is difficult to 'regulate'. Users will not be allowed to choose which laws to apply to the Internet, and which ones to ignore. Freedom online, as the absence of the state, or the protection of Internet users from surveillance by the state is only possible at the cost of permitting the existence of online activities potentially distasteful to a majority of Internet users.

> "It is impossible to hold onto national law successfully and not compromise the transnational openness of the Internet. […T]he transnational Internet and national laws can only be 'reconciled' either by creating a less transnational Internet or more global laws or a bit of both. The globalisation of laws allows the Internet to be retained as an open medium but occurs at the expense of peculiar national laws and values. On the other hand, making the Internet less transnational, through territorial zoning of online activity, allows national policies reflecting peculiar cultural, social and political values to be preserved but at the expense of the uninhibited freedom of transnational online communications."
>
> (Kohl, 2007, pp. 253-254)

In this context, it is no longer "authoritarian governments who are aggressively blocking and censoring the Internet" who are the greatest danger to "the most powerful engine for […] the free exchange of ideas ever invented" (Cox, 2003, p. 3). Instead, 'the most powerful engine for' the change of the status of the Internet are the governments of democratic countries endeavouring to protect their citizens and national economies from harm.

The Internet in 2011

The year 2011 has seen dramatic developments towards the emergence of an Internet of Nations, although the Chinese government remains the only one to talk openly about its plans. Other governments, however, have started to admit that unsupervised Internet freedom is no longer an acceptable state. In the USA, Secretary of State, Hillary Clinton, admitted in a speech that "Internet freedom had to be balanced against a need for security from cyber-criminals and terrorists" (Sheridan, 2011), while in the United Kingdom, prime minister David Cameron announced plans to "prevent people from using" "social media […] to organise […] riots" (Keane, 2011).

Australia's government first introduced plans to censor the Internet accessible to Australians in 2009 (Moses, 2009), ostensibly targeting child pornography. The plan that was partially put into practice in 2011, though, is capable of far more comprehensive censorship, as it uses blacklists of IP addresses installed on the servers of ISPs to limit access to specific sites (Dooling, 2011) – similar to Chinese censorship of its own Internet. Opponents of the plan have argued that the whole process is not transparent enough, and that there is no clear appeals procedure in place to guarantee the protection of innocents, but this did not stop the Australian state.

In May 2011, it emerged that the European Union was harbouring similar plans, and that a proposal had been tabled in January 2011 to introduce 'border controls' on datalinks entering and leaving the European Union. According to the proposal, illicit contents from outside the EU were supposed to be blocked at these border controls (Baker, 2011) and ISPs in the EU member countries were to have received regularly updated blacklists of websites hosting illegal materials (Williams, 2011). While it is doubtful that such a plan could be implemented in the EU with the agreement of enough member countries – in particular during the current economic crisis and its attendant fights within the EU, the tabling of such a proposal indicates that the EU has shifted to a more 'spatial' understanding of the Internet, and is also 'learning' from the Chinese government's approach to the Internet.

In the USA, the year 2011 brought the plan to congress to also employ blacklists to censor the access of its citizens to certain websites. The US plan is far more ambitious than the Australian one, in that different police and security organisations are to be given the power to

add websites to this blacklist that would have to be enforced by all US-based ISPs (N. Anderson, 2011b). This would have the effect of creating a far more comprehensive and secretive censorship system than the Chinese one, which is why many individuals and organisations are protesting against its introduction(N. Anderson, 2011a).

Even more interesting for the topic of this paper is the recent announcement by the United States that they would regard a 'cyber attack' against the USA in the same way as any other 'act of war' and respond accordingly. Due to its limitations in the pursuit of such a war online, the United States would however employ its military forces for retaliation offline (Mulrine, 2011). Although the statements made by US politicians and military officers lacked clarity and would be impossible to apply in the real world (Carr, 2011), they do convey the underlying assumption that the *online* territory of the USA was to be regarded as equivalent to its *offline* territory. Both of these recent developments in the USA, taken in conjunction, serve as additional steps towards a less global, more local Internet.

As a final example of the Internet in 2011, at a meeting of the G8 in Paris, in May 2011, France's president Nicholas Sarkozy lobbied for the regulation of the Internet by national governments. In meetings between executives from several of the largest Internet companies and heads of state, he argued that online freedom might be good for online business, and should therefore be encouraged, but that Internet users and companies profiting from online commerce also needed to "hear our limits, our red lines" (Keaten, 2011). He and other policymakers wanted to strike a balance between promoting legitimate (commercial) uses of the Internet, while preventing abuses of online freedom, identifying this as one of the key challenges to governments for the next few years.

In summary, the year 2011 appears to herald an end to the unrestricted, global Internet – even in government discourses. In (conscious or unintentional?) imitation of the Chinese government and its 2010 White Paper, governments around the world are beginning to claim online spaces as a part of the territory under their jurisdiction and protection. While researchers and Internet users appear more concerned about the power of multi-national Internet companies such as Google, Apple, and Microsoft (see e.g. MacKinnon, 2008), and hope for a protection of the freedom of Internet users from those companies by national governments, the 'take-over' of the Internet by nation states appears to be in full progress – and unstoppable.

Musings about the future

The future of the Internet does not appear quite as rosy and promising as just a few years ago – at least if you are a semi-proficient Internet user of the 'old school' (Lessig, 2004). The easy accessibility of most parts of 'the Internet' and the continuous sensationalist reporting on online events, developments, problems, etc. in the 'traditional' media have turned the Internet into a part of the everyday life of large segments of the populations of most countries in the world. This, in turn, has attracted the attention of governments to the Internet, and to the need to regulate this 'public space'. Whether one sees this as the power-grab of nation states or the legitimate desire of governments to protect their citizens is irrelevant. The consequences are the same, in that the previously unregulated Internet is increasingly becoming regulated. Offline differences in laws, regulations, culture, etc. are in the process projected online, thus also turning the global Internet into an interconnected network of national Intranets with locally different rules.

It is impossible to predict what might happen to 'cross-border' transfers of data in the future, but current efforts by different nation-states to introduce 'border controls' on the connections linking their online spaces to the rest of the world do not bode well. The efforts to combat illegal activities on the Internet through the scanning of all 'inter-national' data packets might hamper the free flow of information online in the same way international air-travel has become increasingly difficult, with its full-body scans, restrictions on items that can be taken along, etc. The Chinese experience shows that websites inside China load up to 10 times faster than websites outside China, resulting in a 95% of all Chinese Internet users not bothering to access the non-Chinese Internet (Roberts, 2011).

While China's treatment of the Internet has long been criticised in the non-Chinese world, and used as an example of an authoritarian government's attempt to oppress its people (e.g. Chase & Mulvenon, 2002), the developments of the past few years are beginning to erode this judgment. China's Internet appears less and less a warning to the 'freedom-loving' people of the world. Instead, the Chinese government's approach to the Internet, both in China and globally, appears to be turning into a model worth emulating for the governments of other nation states. As a result, we might all soon be accessing not the global Internet of the 1990s and 2000s, but instead the *inter-nation-al Internet* of the 2010s – China's contribution to global Internet governance.

References

Anderson, B. R. (1991). Imagined Communities: Reflections on the Origin and Spread of Nationalism (Revised and Extended ed.). London and New York: Verso.

Anderson, N. (2011a). Silicon Valley Congresswoman: Web seizures trample due process (and break the law). Ars Technica Retrieved September 5, 2011, from http://arstechnica.com/tech-policy/news/2011/03/ars-interviews-rep-zoe-lofgren.ars

Anderson, N. (2011b). Why the US needs to blacklist, censor pirate websites. Ars Technica Retrieved September 5, 2011, from http://arstechnica.com/tech-policy/news/2011/04/why-the-us-needs-to-censor-pirate-websites.ars

Arthur, C. (2011). Interviewed: the Turkish hackers whose DNS attack hit the Telegraph. The Guardian Retrieved September 5, 2011, from http://www.guardian.co.uk/technology/2011/sep/05/dns-hackers-telegraph-interview

Baker, J. (2011). Eurpe's 'single secure cyberspace' plan under attack. Computerworld Retrieved September 5, 2011, from http://www.computerworld.com/s/article/print/9216321/Europe_s_single_secure_cyberspace_plan_under_attack

Bandurski, D. (2011). Politics in the age of the microblog. China Media Project Retrieved 2011/08/22, from http://cmp.hku.hk/2011/08/02/14461/

Binoual, I. (2011). Al-Qaeda online presence poses danger. Magharebia Retrieved September 5, 2011, from http://www.magharebia.com/cocoon/awi/xhtml1/en_GB/features/awi/reportage/2011/09/02/reportage-01

Carr, J. (2011). What is Cyberwar? Slate Retrieved September 5, 2011, from http://www.slate.com/id/2301253/

Cartier, C. (2011). Frank Sfarzo, Amanda Knox-Case Blogger, Silenced by Google After Lawsuit by Italian Prosecutor Giuliano Mignini. Seattle Weekly Retrieved September 3, 2011, from http://blogs.seattleweekly.com/dailyweekly/2011/05/frank_sfarzo_amanda_knox-suppo.php

Castells, M. (2010 [1996]). The Rise of The Network Society (Second edition with a new preface ed.). Malden and Oxford:: Wiley-Blackwell.

Chase, M. S., & Mulvenon, J. C. (2002). You've Got Dissent!: Chinese Dissident Use of the Internet and Beijing's Counter-Strategies. Washington D.C.: Rand Corporation.

Chu, W.-C. R., & Cheng, C.-T. (2011). Cultural convulsions: examining the Chineseness of cyber China. In D. K. Herold & P. Marolt (Eds.), Online Society in China: Creating, celebrating, and instrumentalising the online carnival (pp. 23-39). London and New York: Routledge.

Conroe Police Department. (2011). If it's too good to be true, it's probably a scam. Your Houston News Retrieved September 5, 2011, from http://www.yourhoustonnews.com/courier/news/if-it-s-too-good-to-be-true-it-s/article_e4801a18-c375-5660-bde3-62ff0077836d.html

Cox, C. (2003). Establishing Global Internet Freedom: Tear Down this Firewall. In A. Thierer & C. W. Crews, Jr. (Eds.), Who rules the net? Internet governance and jurisdiction (pp. 3-11). Washington D.C.: Cato Institute.

Dooling, A. (2011). Australia Internet to censor over 500 websites. Huffington Post Retrieved September 5, 2011, from http://www.huffingtonpost.com/2011/06/22/australia-internet-censorship_n_882312.html

Dutton, W. H., & Jeffreys, P. W. (Eds.). (2010). World Wide Research: Reshaping the Sciences and Humanities. Cambridge, MA, and London: MIT Press.

Enos, L. (2000). Yahoo! forced to bar French from Nazi auctions. Ecommerce Times Retrieved September 3, 2011, from http://www.ecommercetimes.com/story/3387.html?wlc=1280907310&wlc=1315032685

Fairfax Media. (2011). FBI to support Northern Territory police in hunt for cyberspace sex offenders. Katherine Times Retrieved September 5, 2011, from http://www.katherinetimes.com.au/news/local/news/general/fbi-to-support-northern-territory-police-in-hunt-for-cyberspace-sex-offenders/2281211.aspx

Farrall, K. N., & Herold, D. K. (2011). Identity vs. anonymity: Chinese netizens and questions of identifiability. In D. K. Herold & P. Marolt (Eds.), Online Society in China: Creating, celebrating, and instrumentalising the online carnival (pp. 165-183). London and New York: Routledge.

Fong, C. (2009). 'Sea turles' powering China's Internet growth. CNN Retrieved September 5, 2011, from http://edition.cnn.com/2009/TECH/09/30/digitalbiz.redwired/index.html

Forde, E. (2011). Online piracy is not declining. Music Week Retrieved September 5, 2011, from http://www.musicweek.com/story.asp?sectioncode=1&storycode=1046259&c=1

Herold, D. K. (2008). Development of a Civic Society Online? Internet Vigilantism and State Control in Chinese Cyberspace. Asia Journal of Global Studies, 2(1), 26-37.

Herold, D. K. (2010). Nationalism vs. Democracy – China's bloggers and the Western Media. In S. Yao, W. Bin, S. Morgan & D. Sutherland (Eds.), Sustainable Reform and Development in Post-Olympic China (pp. 171-189). London and New York: Routledge.

Herold, D. K. (2011a). Human flesh search engines: Carnivalesque riots as components of a 'Chinese democracy'. In D. K. Herold & P. Marolt (Eds.), Online Society in China: Creating, celebrating, and instrumentalising the online carnival (pp. 127-145). London and New York: Routledge.

Herold, D. K. (2011b). Netizens and Citizens, cyberspace and modern China. In D. K. Herold & P. Marolt (Eds.), Online Society in China: Creating, celebrating, and instrumentalising the online carnival (pp. 200-208). London and New York: Routledge.

Herold, D. K. (2011c). Noise, spectacle, politics: Carnival in Chinese cyberspace. In D. K. Herold & P. Marolt (Eds.), Online Society in China: Creating, celebrating, and instrumentalising the online carnival (pp. 1-19). London and New York: Routledge.

Information Office of the State Council of the PRC. (2010). The Internet in China. China.org.cn Retrieved 20 August 2011, from http://www.china.org.cn/government/whitepaper/node_7093508.htm

Jackson, P. (2011). England riots: Dangers behind false rumours. BBC News Retrieved September 5, 2011, from http://www.bbc.co.uk/news/uk-14490693

Kaiser, T. (2011). Fedeal Agencies agree to work harmoniously for Cyber Security. Daily Tech Retrieved September 5, 2011, from http://www.dailytech.com/Federal+Agencies+Agree+to+Work+Harmoniously+for+Cyber+Security/article22605.htm

Keane, B. (2011). Back to the future with Cameron's digital riot act. Crikey Retrieved September 5, 2011, from http://www.crikey.com.au/2011/08/12/back-to-the-future-with-camerons-digital-riot-act/

Kearney, C. (2008). U.S. arrests 8 in online sports betting operation. Reuters Retrieved September 3, 2011, from http://www.reuters.com/article/2008/01/07/us-usa-costarica-gambling-idUSN0742137820080107

Keaten, J. (2011). Internet rules at center of 'e-G8' forum in Paris. USA Today Retrieved September 5, 2011, from http://www.usatoday.com/tech/news/2011-05-25-internet-rules-eG8_n.htm

Kennedy, D., & Doran, J. (2006). Gambling chiefs 'at risk of being extradited to US'. The Sunday Times Retrieved September 3, 2011, from http://business.timesonline.co.uk/tol/business/law/article690047.ece

Kohl, U. (2007). Jurisdiction and the internet: Regulatory competence over online activity. Cambridge, New York, Melbourne, Madrid, Cape Town, and Sao Paolo: Cambridge University Press.

Lawson, S. (2001). Judge dismisses French case against Yahoo. PCWorld Retrieved September 3, 2011, from http://www.pcworld.com/article/70323/judge_dismisses_french_case_against_yahoo.html

Lessig, L. (2004). Free Culture. New York: The Penguin Press.

MacKinnon, R. (2008). Silicon Valley's benevolent dictatorship. RConversation Retrieved 22/05/2009, from http://rconversation.blogs.com/rconversation/2008/07/silicon-valleys.html

Marsden, R. (2011). Tweet, tweet! You're fired. IOL SciTech Retrieved September 5, 2011, from http://www.iol.co.za/scitech/technology/internet/tweet-tweet-you-re-fired-1.1130243

McCarthy, M. (2006). U.S. cracking down on offshore betting industry. USA Today Retrieved September 3, 2011, from http://www.usatoday.com/sports/2006-07-18-online-gaming_x.htm

Meng, B. (2011). From Steamed Bun to Grass Mud Horse: E Gao as alternative political discourse on the Chinese Internet. Global Media and Communication, 7(1), 33-51. doi: 10.1177/1742766510397938

Moses, A. (2009). Internet censorship plan gets the green light. The Sydney Morning Herald Retrieved September 5, 2011, from http://www.smh.com.au/technology/technology-news/internet-censorship-plan-gets-the-green-light-20091215-ktzc.html

Mu, X. (2011). Chinese microblog users become strong force to help those in need. Xinhuanet Retrieved 2011/08/22, from http://news.xinhuanet.com/english2010/china/2011-08/04/c_131027672.htm

Mulrine, A. (2011). You hack, we shoot: Pentagon discusses armed counterstrikes to cyberattacks. The Christian Science Monitor Retrieved September 5, 2011, from http://www.csmonitor.com/layout/set/print/content/view/print/399024

Peterson, J. (2011). Internet danger can be reduced. News-Leader Retrieved September 5, 2011, from http://www.news-leader.com/article/20110821/LIFE/108210326/Internet-danger-can-reduced

Roberts, H. (2011). Local control: About 95% of Chinese web traffic is local. The Berkman Center for Internet & Society Retrieved September 5, 2011, from http://blogs.law.harvard.edu/hroberts/2011/08/15/local-control-about-95-of-chinese-web-traffic-is-local/

Ryan, D. J. (2010). Privacy trumps freedom in Italy as Google execs prosecuted. The Business Law Blog Retrieved September 3, 2011, from http://www.dryanlaw.com/privacy-trumps-freedom-in-italy-as-google-execs-prosecuted/

Sheridan, M. B. (2011). Clinton calls for 'serious conversation' about Internet freedom. Washington Post Retrieved September 5, 2011, from http://www.washingtonpost.com/business/economy/clinton-calls-for-serious-conversation-about-internet-freedom/2011/02/15/AB0aUoQ_story.html

So, S., & Westland, J. C. (2010). Red Wired: China's Internet Revolution. London and Singapore: Marshall Cavendish.

Vijayan, J. (2011). DHS warns of planned Anonymous attacks. PCWorld Retrieved September 5, 2011, from http://www.pcworld.idg.com.au/article/399615/dhs_warns_planned_anonymous_attacks

Williams, C. (2011). Alarm over EU 'Great Firewall' proposal. The Daily Telegraph Retrieved September 5, 2011, from http://www.telegraph.co.uk/technology/news/8481330/Alarm-over-EU-Great-Firewall-proposal.html

Xinhua News Agency. (2011). China's microblogs enhance public's supervision of government. Xinhuanet Retrieved 2011/08/22, from http://news.xinhuanet.com/english2010/indepth/2011-08/14/c_131048218.htm