From Cyber Anarchy to Network Control

How the Internet influences State Sovereignty

Annabelle Poelert

3682188

Index

"No frontier lasts forever, and no freely occupied global commons extends endlessly where human societies are involved. Sooner or later, good fences are erected to make good neighbors, and so it must be with cyberspace."[1] *– Demchak & Dombrowski*

1. Introduction

In 2007 Estonia fell victim to a big cyber-attack, blacking out government communication and crashing the online portals of the country's leading banks. The event caused civil unrest and eventually led to riots, leaving 150 people injured and one dead.[2] Three years later, in 2010, Wikileaks started publishing leaked government documents onto the Internet. Among them were war logs and embassy cables that greatly damaged the reputation of the United States (U.S.).[3] The perceived harm of the exposure of these classified documents led some U.S. officials to brand WikiLeaks foreman Julian Assange a terrorist.[4] Around the same time revolutions in Moldova, Iran, Egypt and Tunisia were dubbed "Twitter Revolutions", as revolutionaries made frequent use of Twitter to voice their opinions and organize themselves. Mark Pfeifle, who was a former national security adviser for the U.S. government, praised the social medium for its role in the Iran revolution and proposed to nominate Twitter for the Nobel Peace Prize.[5] During these same Twitter revolutions hackers collective Anonymous played an active role in undermining state censorship and securing communications in Egypt, Iran and Tunisia.[6]

The above-mentioned examples demonstrate how actors can use the Internet as an infrastructure to spread cyber-attacks, secret documents and political ideas. The Internet, a global super network that exists of all interlinked computer networks around the world, supports the fast exchange of information while offering anonymity. Civil society actors take advantage of these characteristics of the Internet to coordinate collective action and activate local protest networks.[7] Their actions on the web could potentially lead to undermining state-authority and state-control. Should states be worried about the Internet eroding their sovereignty?

In this thesis I argue that the opposite is true. Although states are indeed subject to cyber-attacks, cyber security breaches and cyber protests, the Internet at the same time proves to be a medium for state power and control. Take the above examples: by now Estonia has completely

---

[1] C. Demchak and P. Dombrowski, 'Rise of a Cybered Westphalian Age', *Strategic Studies Quarterly* 5 (2011) 1, 32-61, 32.
[2] S. J. Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law', *Berkley Journal of International Law* 27 (2009) 1, 192-251, 193.
[3] B. Keller, 'Dealing with Assange and the Wikileaks Secrets', *New York Times,* 26 February 2011.
[4] J. Cupples and K. Glynn, 'Wikileaks, Illegal Legalities, and the Biopolitics of Collective Counter-intelligence', *Geopolitics* 17 (2012) 3, 681-711, 697.
[5] M. Gladwell, 'Small Change: Why the Revolution Will Not Be Tweeted', *The New Yorker*, 4 October 2014.
[6] Y. Ryan, 'Anonymous and the Arab Uprisings', *Aljazeera,* 19 May 2011.
[7] P. Howard, S. Agarwal and M. Hussain, 'When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media' *The communication Review* 14 (2011) 3, 216-233, 218.

recovered from its online attack and is one of the leading countries in cyber security measures. The country offers most of its governance services online, including the application for virtual citizenship.[8] And even though the reputation of the U.S. government has indeed been damaged by leaked classified documents, these leaks also proved that the U.S. government is leading a large-scale surveillance program in which it taps into and monitors information flows to gain more control over what is happening on the Internet.[9] Lastly, the 'Twitter Revolutions' in the Middle East have not only taught us that social media can play a role in the mobilization of citizens, but also showed that when it is deemed necessary by state authorities the Internet can be taken down altogether, cutting off all access to the Internet.[10]

In short, the cliché of the Internet as an unregulated democratic cyberspace, where states have no influence and control, seems out-dated. States are becoming increasingly aware of the hazards of the Internet and are taking a more pro-active stance on Internet regulation. Ironically enough, they are using the same infrastructure that previously threatened their state authority and control, to re-establish their power. State authorities are exploring ways to erect cyber walls and are collecting data to regain control of the Internet. That is why we are witnessing what Chris Demchak and Peter Dombrowski call "the rise of a cybered Westphalian age", referring to the treaty of 1648 which divided state power according to clear geographic boundaries, guaranteeing self-entitlement and non-interference.[11]

Ever since the rise of the Internet, scholars have argued that the Internet has transformed power structures within society. These arguments have ranged from the state losing control over information flows, to the state being threatened by networks of people mobilizing support through the web.[12] Ten years ago Daniel Drezner wrote the following: "The Internet could be safely described as a tough test for state centric theories of international relations, and an easy test for global civil society arguments."[13] In state centric theories the state is considered the primary political actor in world politics; a role that was perceived to be under pressure by the democratizing effect of the Internet.

In this thesis I will argue that the state centric theories have passed the test, as the Internet has not resulted in the erosion of the political power of the state. I will support this line of reasoning by first giving a short description of the historical context of the Internet. Secondly, I will give an overview of the academic debate amongst political scientists about the influence of the Internet on the

---

[8] E. B. Schnurer, 'E-stonia and the Future of the Cyber State', *Foreign affairs,* 28 January 2015.
[9] G. Greenwald and E. MacAskill, 'NSA Prism program taps in to user data of Apple, Google and others' *The Guardian,* 7 June 2013.
[10] J. D. Sutter, 'The faces of Egypt's 'Revolution 2.0'', *CNN,* 21 February 2011.
[11] Demchak and Dombrowski, 'Rise of a Cybered Westphalian Age', 32.
[12] J. Arquilla and D. Ronfeldt, *The Advent of the Netwar: The Future of Terror, Crime and Millitancy* (Santa Monica 2001) 14, and J. Eriksson and G. Giacomello, 'The Information Revolution, Security, and International Relations: (IR)relevant Theory?', *International Political Science Review* 27 (2006) 3, 221-244, 225.
[13] D. W. Drezner, 'The Global Governance of the Internet: Bringing the State Back in', *Political Science Quarterly* 119 (2004) 3, 477-498, 479.

sovereignty of states. After that, the concept of sovereignty will be demarcated and Steven Krasner's framework on sovereignty will be introduced. Based on Krasner's Framework I will analyse China's and the U.S.' government policies and regulations regarding the Internet. These two case studies were chosen based on the assumption that these states represent two opposites of the political spectrum, with the first being an authoritarian regime and the latter a liberal democracy. Based on my research, I will argue that both authoritarian and liberal states have taken successful measures to control and regulate the Internet and in some cases have even used the Internet to strengthen their sovereignty.

In the case studies I will look at the government policies and regulations regarding controlling and monitoring the Internet based on Krasner's framework of sovereignty. In order to do so, the policies and regulations will be subdivided into the different dimensions of sovereignty as identified by Krasner. In China these types of government interventions are present from the first moment China connected to the Internet in 1994.[14] Therefore I will take 1994 as a starting point for this case study. In the U.S., measures for regulating the Internet were considerably sharpened after the 9/11 attacks.[15] I consider this moment a watershed in U.S. policy because it has helped to shape a discourse of war, which allowed the U.S. government to implement policies and regulations that focussed on regaining control of the Internet. The starting point for the analysis of the U.S. case study will therefore be 2001. Because many of the legislation and policies are complementary and subject to constant change I have chosen not to structure the case studies in chronological order, but to structure them according to Krasner's dimensions of sovereignty. This way of organizing allows the structural comparison of policies and regulations and their effectiveness in both countries.

For the outline of the academic debate, the demarcation of sovereignty as a concept, and the introduction of Krasner's framework, I will conduct a literature study. For my case studies I will rely on both scientific articles and primary sources, such as policy documents, political blogs, newspaper articles and human rights reports. As the case studies focus on the past 25 years of Internet policy, much of the official Chinese and U.S. policy documents are still classified. I will therefore complement available policy documents with other types of primary and secondary sources in order to be able to provide a comprehensive overview of policies and regulations regarding the Internet and their effectiveness.

For the case study on China the language barrier requires this research to rely on translations of official policy documents (mostly provided by the Chinese government itself) and political blogs. For the case study on the U.S., frequent use is made of articles that appeared in *The Guardian* and *The New York Times*. Both newspapers have published a selection of leaked official documents by Edward

---

[14] G. Walton, *China's golden shield: corporations and the development of surveillance technology in the People's Republic of China* (Quebec, 2001), 9.
[15] Department of homeland Security, 'Safeguarding and Securing Cyberspace', *Department of Homeland Security* (version: 19 January 2016) https://www.dhs.gov/safeguarding-and-securing-cyberspace (9 March 2016).

Snowden, accompanied with background articles that give insight in measures that the U.S. government took to regain control of the Internet. This allows the case studies to make use of sources that are not officially unclassified yet. However, it is important to take into account that research journalists handpicked their material from a great amount of classified documents. Inevitably this means that this research has to rely on the choices that these journalists have made on which information is important to make publicly available and their way of presenting the facts.

2. The academic debate

Since Tim Berners-Lee created the World Wide Web in 1990, Internet scientists have debated the profound effects that the Internet would have on politics. With the rise of the Internet the foundation was laid out for an entirely new infrastructure of society. Not only did it become possible to complete transactions in milliseconds, influencing the world's economic system, but the Internet also enabled people to interact with others across the globe in ways that were previously unheard of. The Internet provided humans with a platform and a way to interconnect, regardless of space and time, enabling people to organise themselves in entirely new ways. This led many to believe that the Internet would have a democratizing effect on society.[16]

While in the early 1990s the use of the Internet started to rise rapidly, social scientists tried to forecast the kind of transformation society would go through as the inevitable result of this new information infrastructure. The famous social scientist Manuel Castells envisioned a world in which the rigid borders of states would, under the influence of the Internet, slowly disappear. Instead, the world would be made up of flows of people, goods and services, coming together in hubs and nodes in what he calls the 'network society'.[17] Many other scientists followed in his footsteps, predicting the end of the nation state and forecasting that the state would eventually be replaced by other entities that were deemed more suitable to fit the needs of a globalized society.[18] In short, it was believed that the rise of the Internet would erode state sovereignty, potentially even challenging the legitimacy of the state as the highest territorial authority.

Yet others have argued that the rise of the Internet has had a negligible effect on the political realm of states. Even more so, when 'rightly' used, the Internet could constitute a powerful tool for domestic surveillance and could lead to the state exerting more control in its territory than ever before.[19] Although these scientists admit that state power is increasingly decentralized, they explain the decentralization of state power to NGO's and private companies and the formation of global

---

[16] P. Ferdinand, 'The Internet, democracy and democratization', *Democratization* 7 (2000) 1, 1-17, 2.
[17] M. Castells, *The Rise of the Network Society* (Sussex 2010), xiii.
[18] J. Lea and K. Stenson, 'Security, Sovereignty and Non-State Governance "From Below"', *Canadian Journal of Law and Society* 22 (2007) 2, 9-27, 9.
[19] M. Hathaway, 'Connected Choices: How the Internet is Influencing Sovereign Decisions', *American Foreign Policy Interest* 36 (2014) 5, 300-313, 306.

policies as a conscious choice of the state. In other words, the state can decide what is political and what is not. Janice Thomson calls this 'meta-political authority' and sees it as an essential part of state sovereignty.[20] As this argument leaves the authority of decision-making at the state level intact, this implies that state sovereignty has not been affected by the rise of the Internet.[21]

The academic debate about the rise of the Internet and its influence on state sovereignty can be simplified to two diametrically opposed strands of thought. The first is that the rise of the Internet has eroded state sovereignty. The second is that the rise of the Internet has not substantially affected the sovereignty of states and in some cases might even have strengthened it. These two strands of thought are roughly overlapping with two major schools of thought within International Relations: respectively Liberalism and Realism.[22] Both have come up with convincing arguments that support their perception of reality and it is important to have a closer look at both discourses, as it will only be possible to conduct a meaningful case study that will contribute to the debate, when both ways of reasoning are fully understood.

David Bollier falls into the first category of scholars who believe that the Internet is responsible for the erosion of state sovereignty. He argues that non-state actors are winning terrain in the previously exclusive domain of state power. Bollier is convinced that many features of state sovereignty, like participation in international politics and control of transnational communications, have been taken over by other political entities, amongst them NGOs, ethnic communities and even individuals.[23] Furthermore he believes that the Internet has played a key role in facilitating this process. The Internet provided non-state actors with a global platform through which they could organize themselves. Through cyber campaigns they have found ways to exert political and economic influence.[24] This is in line with Melissa Hathaway's view, who sees the Internet "as an instrument of power projection and military capability" that "challenges traditional ideas of security, stability, and sovereignty."[25]

Saskia Sassen agrees with this point of view and calls the Internet "a powerful medium for non-elites to communicate, support each other's struggles and create the equivalent of insider groups at scales going from local to global."[26] John Aquilla and David Ronfeldt share this thought and state that the very nature of the Internet results in a transfer of power from states to non-state actors. In contrast

---

[20] J. E. Thomson, 'State Sovereignty in International Relations: Bridging the Gap between Theory and Empirical Research', *Internal Studies Quarterly* 39 (1995) 2, 213-233, 214.
[21] Drezner, 'The Global Governance of the Internet', 478.
[22] S. Sassen, 'The Impact of the Internet on Sovereignty: Unfounded and Real Worries', in Christoph Engel and Kenneth H. Keller (eds.), *Understanding the Impact of Global Networks on Local Social, Political and Cultural Values* (Baden-Baden: Nomos, 2000), 195-201, 196.
[23] D. Bollier, 'The Rise of Netpolitik – How the Internet is Changing Politics and Diplomacy' (Version 2003), http://bollier.org/sites/default/files/aspen_reports/NETPOLITIK.PDF (03 January 2016) 1.
[24] Bollier, 'The Rise of Netpolitik', 1.
[25] Hathaway, 'Connected Choices', 301.
[26] Sassen, 'The Impact of the Internet on Sovereignty', 201.

to the traditional hierarchical structure of the state, non-state actors often have a more dynamic organisation structure, connecting themselves through nodes and channels, which make them more suitable for the Internet.[27] Concrete examples are terrorist groups, who use the Internet to communicate and to coordinate dispersed activities.[28] Through the Internet, groups with similar ideologies can form ties and plan terrorist attacks on an ad hoc basis. This results in very dynamic networked organisations, making it hard to establish how terrorist groups are interlinked.[29]

According to Nazli Choucri and Daniel Goldsmith not only state structures are less suitable for the Internet, but also their traditional security policies are a mismatch for cyberspace. Choucri and Goldsmith argue that until the end of the Cold War national security policies were stooled on deterrence, a strategy that is not easy to transfer to the cyber domain. They state that destabilizing cyber threats make it necessary for governments to reform national security policies to be able to guarantee the safety of their citizens.[30]

Apart from direct challenges to states, like terrorist organisations or cyber threats, the Internet has also had a more indirect influence on state sovereignty by eroding state control on information flows.[31] Choucri and Goldsmith warn that the Internet "allow[s] almost anyone to disseminate messages, meaning that a wide range of actors, state and non-state, have the potential to disrupt networks and commerce with relatively little fear of discovery."[32] The relative anonymity of the Internet makes it easier to speak out against the authorities and to mobilize people for your cause.

Eriksson and Giacomello confirm that the Internet is a powerful communication tool that is used by news media, NGOs and individuals to spread non-governmental information, to distribute independent reports and to make counterclaims.[33] While states previously had the capabilities to control and censor what information was spread within its borders, the speed with which information is disseminated and the complexity of the Internet have made it nearly impossible to monitor information flows. Some political scientists would argue that this loss of control over information flows would directly endanger national security and erode state sovereignty.[34]

Melissa Hathaway gives a concrete example of this by describing the influence of the freely available software called The Onion Router (TOR). Volunteers maintain this open network and enable communications and content to circumvent blocks on the Internet. At the same time the use of relays

---

[27] J. Arquila and D. Ronfeldt, *Networks and Netwars: The future of Terror, Crime and Militancy* (Santa Monica 2001) 1.
[28] Arquila and D. Ronfeldt, *Networks and Netwars,* 29.
[29] J. Eriksson and G. Giacomello, 'The Information Revolution, Security, and International Relations: (IR)relevant Theory?', *International Politcal Science Review* 27 (2006) 3, 221-244, 227.
[30] N. Choucri and D. Goldsmith, 'Lost in cyberspace: Harnessing the Internet, international relations, and global security' *Bulletin of Atomic Scientists* 68 (2012) 2, 70-77, 71.
[31] Eriksson and Giacomello, 'The Information Revolution, Security, and International Relations', 224.
[32] Choucri and Goldsmith, 'Lost in Cyberspace', 70.
[33] Eriksson and Giacomello, 'The Information Revolution, Security, and International Relations', 227.
[34] Ibidem, 227.

increases security and privacy and guarantees anonymity for the users of TOR. According to Hathaway there are liberal governments who facilitate TOR to enable freedom of speech and to promote their democratic values across the world. These governments are accused of indirectly interfering in the sovereign business of other states.[35]

This line of thought resonates with what Bollier calls 'the rise of netpolitik'. He describes how politics in the arena of the Internet is not so much about the display of coercive power, but about softer issues, like who can claim moral legitimacy.[36] Bolliers writes that "[p]ower in the global information society depends less on territory, military power, and natural resources. Rather, information, technology, and institutional flexibility have gained importance in international relations. The power of knowledge, beliefs, and ideas are the main tools of political actors in the effort to achieve their goals."[37] In short, he argues that power is no longer in the hands of the actor that has the biggest military strength but in the hands of the actor that can best orchestrate public sentiment.

Daniel Drezner disagrees with the above line of reasoning and belongs to the second group of scholars, claiming that the Internet has not eroded state sovereignty. He believes that states remain the primary actors in a globalizing world, as they are still the most successful in achieving their preferences vis-à-vis non-state actors. According to Drezner "Non-state actors can still influence outcomes on the margins, but their interactions with states are more nuanced than the globalization literature suggest."[38] Drezner also believes that there are plenty examples of states regulating the content that is accessible from within their borders. Although he admits that these state efforts are never 100 per cent effective, they are nevertheless sufficient to speak of cyber regulation.[39]

Other political scientists agree with this Realist view and claim that the Internet is becoming increasingly territorialized by states. Demchak and Dombrowski argue that we can already witness the beginnings of a border-making process on the Internet. According to them it's not just autocratic states that are consolidating their power on the web, but also democratic states, which erect borders on the net in name of security.[40] In their article they suggest the following: "While it is not recognized as such nor publicly endorsed by most democratic leaders, a cyberspace regulating process is happening, building the initial blocks of emergent national virtual fences."[41]

Demchak and Dombrowski go even further by stating that not only borders will arise in cyberspace, but that they will also be defended by militaries – or at least their cyber equivalent.[42] This goes against the idea of the Internet being primarily the arena of soft power, as Bollier had described

---

[35] Hathaway, 'Connected Choices', 306.
[36] Bollier, 'The Rise of Netpolitik', 2.
[37] Bollier, 'The Rise of Netpolitik', 4.
[38] Drezner, 'The Global Governance of the Internet', 478.
[39] Ibidem, 488.
[40] Demchak and Dombrowski, 'Rise of a Cybered Westphalian Age', 32.
[41] Ibidem, 35.
[42] Ibidem, 35.

it, and paints a picture of the cyber domain as a virtual extension of the state and thus state sovereignty. Demchak and Dombrowski's view is supported by the 2011 U.S. cyber strategy in which one of the five strategic initiatives is to "treat cyberspace as an operational domain to organize, train, and equip so that the [Department of Defence] can take full advantage of cyberspace's potential."[43] Even more so, the traditional policy of deterrence that Choucri and Goldsmith deemed unfit for the virtual world has a prominent place in the U.S. cyber strategy for 2015, which says: "Deterrence is a key part of the [Department of Defence]'s new cyber strategy. This strategy describes the Department of Defense (DoD) contributions to a broader national set of capabilities to deter adversaries from conducting cyberattacks."[44]

Apart from discussion about the extension of state regulation into cyber territory, political scientists also disagree on the role of private actors on the Internet. While some scientists believe that private actors challenge state sovereignty, Jeremy Crampton believes that private actors actually extend state control.[45] According to Crampton the interests of governments and private organisations often overlap. The result is government-corporate partnerships that, as in the case with the mass surveillance programs of the NSA, lead to governments gaining access to the data that are owned by private actors.[46] It is almost as if the government is outsourcing its data collection practices to private corporations. Furthermore it seems naïve to think that private actors have any choice but to turn over their data to governments. As the leaked documents by Snowden show, governments can gain access to servers by issuing warrants.[47]

Lastly, Janice Thomson argues that we are not witnessing the erosion but the transformation of sovereignty. This new form of sovereignty has more emphasize on prevention than on regulation. It includes extensive methods of surveillance, which is partly outsourced to private companies who have mastered subtle techniques of surveillance. The result is a complex relationship between public and private actors, in which the state has the final authority.[48]

To summarize, according to the scholars on one side of the debate, the Internet has become a vehicle for non-state actors to defend their interests and to gain influence in the political and economic sphere. They believe that the complex nature of the Internet makes it hard to censor information and to

---

[43] Department of Defence, 'Department of defence strategy for operating in cyber space' (Version July 2011) http://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD%20Strategy%20for%20Operating%20in%20Cyberspace%20July%202011.pdf (31-11-2015).
[44] Department of Defence, 'Fact sheet: The department of defence (DoD) cyber strategy', (version: April 2015) http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf (31-11-2015).
[45] J. Crampton, 'Collect it All: National Security , Big Data and Governance', *GeoJournal* 80 (2015) 519-531, 520.
[46] Greenwald and MacAskill, 'NSA'.
[47] Crampton, 'Collect it all', 523.
[48] Thomson, 'State Sovereignty in International Relations', 226.

trace back data to its source, resulting in a loss of control over information flows. Terrorist groups, diaspora and civil society use the Internet to mobilize people for their cause, which can eventually result in threats to state security and sovereignty. Especially in a time in which power is influenced by legitimacy, the use of the Internet is a new battleground on which the state meets its challengers. Furthermore most information flows are owned by private actors, who collect and store data, and who, by doing so, have entered a domain that traditionally belonged to the state.

The scholars on the other side of the debate argue that the state is increasingly establishing its authority in cyberspace by extending sovereign policies and practices to the virtual world. They believe that the state has not lost its authority but has found ways to outsource certain control mechanisms to non-state actors. These complex private-public partnerships enable states to strengthen their authority and control over society.

2.1 Demarcating the concept of state sovereignty

The essence of the scholarly debate about the rise of the Internet and its impact on political society is about state sovereignty - to what extent has the position of the state as prime political entity been eroded? Before determining the relationship between state sovereignty and the Internet, it is important to demarcate the concept of state sovereignty. A quick glance at the literature on this matter reveals that the definition of state sovereignty is far from straight forward and is adding another layer of complexity to this scholarly debate. It is therefore necessary to decompose the notion of state sovereignty and to look into the impact of the Internet on all its different facets. It will only be possible to come to a meaningful conclusion about the impact of the Internet on state sovereignty when all different elements of state sovereignty are identified.

Although most scholars seem to agree that the origin of state sovereignty lays at the peace of Westphalia in 1648, it is widely disputed what the concept of sovereignty actually encompasses. In their article about cyber threats and security, Eriksson and Giacomello define state sovereignty as 'effective control of the national territory and of the people living within it'.[49] Scott Shackelford, however, argues in his article on cyber warfare that state sovereignty should be 'conceived not as an application of state control but of state authority'.[50] These two different interpretations of state sovereignty show the difference in focus of two major schools of thought in international relations and exemplify the complexity of the debate.

While the liberalists put emphasis on the aspect of state control as indicator of state sovereignty, realists focus on the aspect of state authority. As Thomson proclaims "Given the two schools' focus on these different aspects of sovereignty, it is not surprising that International Relations theorists make conflicting and sometimes diametrically opposed claims about the status of sovereignty

[49] Eriksson and Giacomello, 'The Information Revolution, Security, and International Relations', 224.
[50] Shackelford, 'From Nuclear War to Net War', 215.

in the post-Cold War era".[51] In order to come to a comprehensive understanding about the influence of the Internet on state sovereignty, it is therefore important to keep these different starting assumptions in mind and to come up with a definition of state sovereignty that would satisfy both schools of thought.

In short, the definition of sovereignty as it will be used in this research needs to at least reflect both state control and state authority. One of the most comprehensive frameworks of state sovereignty comes from Stephen Krasner. Krasner's interpretation of sovereignty takes into account the aspects of authority and control, meeting the requirements of both liberalist and realist thinkers. It therefore provides an excellent framework to use in determining the relation between the rise of the Internet and state sovereignty. As Krasner makes a distinction between different dimensions of sovereignty, it becomes possible to divide and analyse measures that states have taken within each dimension of sovereignty.

Krasner identifies four different dimensions of sovereignty: domestic sovereignty, interdependence sovereignty, Westphalian sovereignty, and international legal sovereignty.[52] The first two dimensions of sovereignty have to do with the control that the state exercises across its territory, while the latter two dimensions of sovereignty are more focused on the authority of the state.[53] I will now provide a more comprehensive overview of Krasner's four dimensions of sovereignty.

Domestic sovereignty

Domestic sovereignty is about how public authority is organized within a state and about how effective it is.[54] How is the state authority organized? Can the state authority effectively control the people and the developments within its own border? According to Drezner, one of the accepted wisdoms of this time is that globalization, and with it the Internet, 'undercuts state sovereignty, weakening the governments' ability to effectively regulate their domestic affairs'.[55] This perception relates directly to domestic sovereignty, but not to the other dimensions of sovereignty as described by Krasner per se.

According to Edward Luck, domestic sovereignty requires both authority and control, which in turn are deeply related to perceptions of legitimacy.[56] Although Krasner doesn't explicitly includes the concept of legitimacy in his definition of domestic sovereignty, it would be hard to apply the term domestic sovereignty without taking into account to which extent the people of a nation perceive their government as legitimate. Domestic sovereignty can therefore be maintained, both through hard power

---

[51] Thomson, 'State Sovereignty in International Relations', 213.
[52] S. D. Krasner, *Sovereignty, Organized Hypocrisy* (Princeton 1999), 9.
[53] Krasner, *Sovereignty, Organized Hypocrisy,* 10.
[54] Krasner, *Sovereignty, Organized Hypocrisy*, 11.
[55] Drezner, 'The global governance of the internet', 480.
[56] E. C. Luck, 'Sovereignty, Choice and the Responsibility to protect', *Global responsibility to protect* 3 (2009) 1, 10-21, 12.

–police control and the rule of law- and through soft power – influencing public opinion and claiming legitimacy.

The capacity of the Internet to erode state sovereignty is reflected in the amount of states that try to restrict their citizen's access to information on the web.[57] David Betz and Tim Stevens identify three forms of control that states apply on the Internet to secure domestic sovereignty. These three forms of control are broadly defined as the establishing Internet legislation, the manipulation of Internet traffic, and inducing cognitive change.[58] All three forms of control as defined by Betz and Stevens will be accounted for in this thesis.

Interdependence sovereignty

Interdependence sovereignty describes the extent of control that a state authority has when it comes to its geographical boundaries.[59] Can the state control the influx of people, goods, services and information? How porous are its borders? Again it seems to be a conventional wisdom that globalization erodes this control.[60] Internet activist John Perry Barlow suggests that "[b]y creating a seamless opined global economic zone, borderless and uncontrollable, the Internet calls into question the very idea of the nation state."[61]

Although there are plenty of examples that show that states can actually still secure some extent of border control in cyberspace, Barlow's interpretation of sovereignty is unmistakable related to Krasner's definition of interdependence sovereignty. Again, the erosion of this meaning of sovereignty does not necessarily affect the other three meanings of sovereignty.

Westphalian sovereignty

Westphalian sovereignty is based on two basic principles: territoriality and the principle of non-intevention in domestic affairs. This type of sovereignty assumes that the state is the sole legitimate actor within its geographical boundaries.[62] According to Krasner, Westphalian sovereignty can be affected in two ways: by invitation or by intervention.[63] If a country voluntarily gives up a piece of its authority through participation in a supranational organisation its Westphalian sovereignty is compromised by invitation. When an external actor coercively influences the domestic authority structure of a country, its Westphalian sovereignty is compromised by intervention.[64] Westphalian

---

[57] D. Betz & T. Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power* (London 2011), 65.
[58] Betz & Stevens, *Cyberspace and the State,* 65.
[59] Krasner, *Sovereignty, Organized Hypocrisy*, 12.
[60] Ibidem, 12.
[61] J. P. Barlow 'Thinking locally, acting globally', *Time,* 15 January 1996. in: Drezner, 'The global governance of the internet', 480.
[62] Krasner, *Sovereignty, Organized Hypocrisy*, 20.
[63] Ibidem, 13.
[64] Krasner, *Sovereignty, Organized Hypocrisy*, 20.

sovereignty is closely related to state authority and therefore according to Janice Thomson to the power to decide what is political and what is not.[65]

When external actors influence a state's political affairs, one can speak of a violation of Westphalian sovereignty. Shackelford is concerned about the erosion of the Westphalian sovereignty of the nation state and not per se the domestic sovereignty when he writes the following: "[t]ransnational cyberspace activities that affect the internal affairs of a state might breach general legal principles upholding respect for sovereignty and non-intervention."[66]

International legal sovereignty.

International legal sovereignty is about the judicial status of a state; the recognition of the state by external political entities. This type of recognition is important for states as it provides them with material and normative resources.[67] International legal sovereignty entitles states to enter into treaties and alliances. When a state is recognized as such, other states have to respect its independence and juridical equality.[68]

Even though international legal sovereignty - the external recognition of statehood – is a key component of state sovereignty, it is the only meaning of sovereignty that is not directly affected by the rise of the Internet. Eriksson and Giacomello analyze that '[c]yber-threats challenge primarily internal sovereignty (effective control of the national territory and of the people living within it), but not necessarily external sovereignty (the formal recognition of independence by other states)'.[69] David Betz and Tim Stevens agree to this and claim that cyberspace doesn't affect international legal sovereignty "in any substansive sense"[70]. The influence of the Internet on International Legal sovereignty will therefore not be analysed in this research. The other three dimensions of sovereignty will be applied to the case studies of China and the U.S..

3. China and the rise of the Internet

[65] Thomson, 'State Sovereignty in International Relations', 214.
[66] Shackelford, 'From Nuclear War to Net War', 234.
[67] Krasner, *Sovereignty, Organized Hypocrisy*, 16.
[68] Ibidem, 14.
[69] Eriksson & Giacomello 'The Information Revolution, Security, and International Relations', 227.
[70] Betz & Stevens, *Cyberspace and the State,* 73.

"Across the Great Wall we can reach every corner of the world", was the title of the first e-mail that was sent from China in 1987.[71] The message came from two Chinese scientists who had set-up the first e-mail node in the country. Little did they know that a new Great Wall would be erected, this time in cyberspace. Ever since China connected to the Internet in 1994, one of the prime objectives of the Chinese government has been to regulate Internet access and its Internet security strategy has focused on limiting the international connectivity of its citizens to a bare minimum.[72] In order to do so, the Chinese government was actively involved in creating the architecture of the Chinese Internet and has implemented a wide range of cyber policies and cyber regulation programs.

Since 1994 the amount of Chinese citizens with access to the World Wide Web has been steadily growing. In 2013 it was estimated that around 50 per cent of China's inhabitants were connected to the Internet, making the country home to the largest share of Internet users worldwide.[73] The widespread Internet usage amongst Chinese citizens in combination with the restrictive Internet regulations of the Chinese authorities makes China an excellent case study to research how authoritarian states secure their state sovereignty in the age of the Internet.

During the past decennia, the Chinese authorities have taken several different measures to secure their state sovereignty from the potential harm of the Internet. These measures have ranged from censoring the Chinese Internet to lobbying for reforms in the multi-stakeholder model of the Internet. In this chapter I will look at the different measures that the Chinese government has taken since 1994 to secure its domestic sovereignty, interdependence sovereignty and Westphalian sovereignty. Based on these findings I will conclude with analysing to what extent China has been able to secure its sovereignty in each dimension of Krasner's framework.

3.1 The influence of the Internet on China's domestic sovereignty

The relation between domestic sovereignty and the Internet has been a hot topic in China for the past couple of years. According to the Chinese Media Project, an initiative of the University of Hong Kong, *wangluo zhuquan* – translated as Internet sovereignty - has proven to be a real buzzword in Chinese media since 2011.[74] The Chinese Media Project states on its website that "[u]nder the principle of Internet sovereignty […] China reserves the right to control the flow of information on the

---

[71] J. Florcruz & L. Seu "From Snail Mail to 4G, China Celebrates 20 Years of Internet Connectivity" *CNN* (version: 24 April 214) http://edition.cnn.com/2014/04/23/world/asia/china-internet-20th-anniversary/ (24 December 2015).
[72] Walton, *China's golden shield,* (page no. unkown).
[73] M. Svensson, "Internet in China and its Challenges for Europe: Dealing with Censorship, Competition and Collaboration." *ECRAN* (version: August 2014) http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=4935884&fileOId=5044735 (2 Februari 2016), 2.
[74] China Media Project, 'Internet Sovereignty' http://cmp.hku.hk/2015/09/30/39279/ (24 December 2015).

Internet within its borders."[75] But what measures does the Chinese government take to secure its domestic sovereignty on the Internet? And to what extent is it successful in regulating the Chinese citizens in cyberspace?

Law and cyber legislation

When China connected to the Internet in 1994, the Chinese government realized that the Internet posed a grave threat to its authoritarian regime by potentially exposing people to new political ideas. One of the most straightforward ways of minimizing this threat was by creating extensive legislation on Internet behaviour. According to a Human Rights Watch report, the Chinese government issued over sixty sets of regulations between 1995 and 2001 with the aim to control Internet content.[76] These sets of regulations specified which actions on the Internet were considered illegal, making use of opaque terms, like: "spreading information that incites hatred; subversive acts aimed at overthrowing the state; and divulging state secrets."[77] From 2001 onwards, the stealing and/or spreading of state secrets via the web was considered cyber espionage and was treated as a capital crime, which could lead the offender to face the death penalty.[78]

The Internet legislation that has been passed by the Chinese government has been notorious for its vagueness. In 2010 the government published a White Paper, which stated:

> [Chinese laws and regulations] clearly prohibit the spread of information that contains contents subverting state power, undermining national unity, infringing upon national honor and interests, inciting ethnic hatred and secession, advocating heresy, pornography, violence, terror and other information that infringes upon the legitimate rights and interests of others.[79]

As this translation of the white paper reaffirms, these forbidden acts are very multi-interpretable and can be easily used as a ground to make a case against dissidents. This vagueness has enabled the government to arrest people for acts that in the Western world would be considered to be freedom of speech, like publishing critical articles or circulating pro-democratic information.[80]

---

[75] China Media Project, 'Internet Sovereignty'.
[76] Human Rights Watch 'Freedom of expression and the Internet in China', (Version: 1 August 2001) https://www.hrw.org/report/2001/08/01/freedom-expression-and-internet-china (26 December 2015), 1.
[77] L. Tsui, 'The Panopticon as the Antithesis of a Space of Freedom: Control and Regulation of the Internet in China' *China Information* 17 (2003) 65-82, 69.
[78] Human Rights Watch 'Freedom of expression and the Internet in China', 5.
[79] Information Office of the State Council of the People's Republic of China, 'White paper (IV) – Basic Principles and Practices of Internet Administration', (version: 8 June 2010) http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207983.htm (26 December 2015).
[80] Walton, *China's golden shield,* 5.

The regulation of the Internet has become even stricter since Xi Jinping came into office in 2013. He emphasised the strategic importance of regulating the Internet by calling the Internet an "ideological battlefield".[81] Right after he started his precedency he appointed and chaired an Internet security group that would focus on defining the Chinese Internet strategy. Since then, Xi has passed several new laws that enabled the government to prosecute people for minor web based offences, like the spreading of online rumours, which have a maximum sentence of three years imprisonment.[82]

The Chinese government has used different tactics to refrain people from posting critical thoughts on the Internet. One of these tactics is described by Lokman Tsui, who believes that the Chinese Internet regulation is so opaque that people don't know which acts will lead to legal prosecution and which won't. This, in combination with some firm examples of people being prosecuted on grounds of their Internet behaviour, leaves the Chinese people in constant fear of being monitored while using the Internet. According to Tsui this has led to a situation in which people are regulating their own Internet behaviour as if a government official is watching their every move.[83]

Apart from targeting people directly, Chinese legislation on the Internet also targets organisations. In August 2015 China published its draft cyber security law. In line with older legislation, the new law held private operators responsible for regulating the content of the web.[84] A report of Human Rights Watch on the cyber security law shows the extent of government control exercised through this law:

> The draft law requires Internet companies to demand that users provide their real name and personal information (art. 20). It also requires companies [...] to censor undefined "prohibited" messages, stop their spread, cease providing services to the offenders, and report the incidents to the authorities (arts. 40-43). Companies can be fined, their licenses cancelled, and businesses closed if they fail to comply with these requirements (arts. 53 and 57). [85]

Where individuals can't be stopped to post or access information that the regime classifies as illegal, service providers are responsible for deleting illegal content and stopping it from disseminating on the Internet, risking the loss of their licenses if they don't.

---

[81] Svensson, 'Internet in China and its Challenges for Europe', 1.
[82] BBC NEWS 'China Issues new internet rules that include jail time', (version: 09 September 2013) http://www.bbc.com/news/world-asia-china-23990674 (26 December 2015).
[83] Tsui, 'The Panopticon as the Antithesis of a Space of Freedom', 69.
[84] Human Rights Watch, 'Freedom of expression and the Internet in China', 4.
[85] Human Rights Watch, 'Submission by Human Rights Watch to the National People's Congress Standing Committee on the draft Cybersecurity Law' (Version: 4 August 2015) https://www.hrw.org/sites/default/files/supporting_resources/hrw_submission_draft_cybersecurity_law_082015.pdf (26 December 2015).

Large-scale monitoring and surveillance

In 2000 the Chinese government launched Operation Golden Shield, a project that had been developed in the 90's by the Ministry of Public Security (MPS). The operation was set-up to control the content of the Internet, while opening up to ICT and Western innovations. But operation Golden Shield went even further, it was supposed to become an all-encompassing surveillance project that would make use of modern ICT techniques to combine data on citizens. Greg Walton writes that the ultimate aim of the MPS was "the adoption of advanced information and communication technology to strengthen central police control, responsiveness, and crime combating capacity" and that Bejing envisioned "a database driven remote surveillance system – offering immediate access to registration records on every citizen in China, while linking to vast networks of camera's [...]"[86] In the end, the rapid expansion of Chinese Internet usage led to the MPS having to adjust the operation, placing more focus on censorship than surveillance, but the idea to use ICT to create a mass surveillance system lived on.[87]

Recently the focus on online surveillance programs has been restored. The Chinese government has started a pilot to set-up a social crediting system that makes use of online payment systems to judge citizens on their creditworthiness and trustworthiness.[88] Apart from approving government credit services, this system supplies the government with an infrastructure that would enable it to control its citizens by "rating" them based on their (online) behaviour, their consumer habits, and their social network, potentially becoming a system of mass surveillance.[89] As the social credit system will not be officially launched before 2020, the influence of the system on maintaining domestic sovereignty will remain speculation. The pilot, however, is already running and shows that the Internet, viewed by many as a powerful tool for the empowerment of ordinary citizens, can become a powerful tool for the control repression of the same ordinary citizens when in the hands of governments.

Outsourcing cyber regulation to private corporations

The Chinese government is greatly dependent on both national and international private organisations in regulating the domestic cyberspace.[90] As mentioned above, private organisations are required to

---

[86] Walton, *China's golden shield,* 15.
[87] P. Punyakumpol, "The great Firewall of China: Background" *Torfox: A Stanford Project* (Version: 01 June 2011) http://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/author/pingp/index.html (27 December 2015).
[88] C. Hatton, 'China 'Social Credit'; Beijing sets up huge system' *BBC News* (Version: 26 October 2015) http://www.bbc.com/news/world-asia-china-34592186 (24 December 2015).
[89] J. Fan, 'How China wants to Rate its Citizens' *The New Yorker* (03 November 2015) http://www.newyorker.com/news/daily-comment/how-china-wants-to-rate-its-citizens (24 December 2015).
[90] R. Mackinnon, 'Networked Authoritarianism in China and Beyond: Implications for global Internet freedom', *Liberation Technology in Authoritarian Regimes* (Version: 11 October 2010), http://iis-db.stanford.edu/evnts/6349/MacKinnon_Libtech.pdf (03-02-2016), 15.

regulate web content by Chinese law. If they fail to do so, this may lead to the loss of their operating license. Rebecca Mackinnon, Internet freedom advocate, writes: "In this way, much of the censorship and surveillance work is delegated and outsourced by the government to the private sector – who, if they fail to censor and monitor their users to the government's satisfaction, will lose their business license and be forced to shut down."[91]

This brings private corporations in a difficult situation. On the one hand they will need to comply with ever changing forbidden topics that are imposed by the MPS and self-censor their search engines, platforms and websites accordingly. On the other hand the Chinese market with over 600 million Internet users is an attractive commercial opportunity to expand business and services. One of the most cited examples is Google, which, in the past, has censored search queries with sensitive keywords in China.[92] In the end it's often commercial interests that prevail above political interests of large multinationals.

Apart from Google, there are multiple examples of private organisations that have actively contributed to the heavy restrictions on free Internet access by supplying the Chinese government with information technologies for content filtering and mass surveillance systems. The Canadian telecom provider Nortel Networks has played a key role in providing the Chinese authorities with a sophisticated system that is able to filter content at the individual user-level.[93] The American based corporation Cisco played has provided the Chinese government with parts of the necessary infrastructure for Operation Golden Shield.[94]

Furthermore, the Chinese government is now cooperating with eight Chinese companies to pilot the social credit scoring system that was mentioned above.[95] One of the companies participating in the pilot is Alibaba, the world's biggest e-commerce platform, which stated in a press release that it is planning to make use of big data to create credit scores based on people's purchase behaviour and credit history, but also on people's "personal characteristics" and "Interpersonal relationships".[96] By doing so, it provides the Chinese government with knowledge and tools that potentially allow it to exert even more control over its citizen's (web) behaviour.

Another example of the Chinese government's close cooperation with private organisations is the access of the government to all data streams of Telecom and Internet service providers operating in

---

[91] Mackinnon, 'Networked Authoritarianism in China and Beyond', 15.
[92] The Economist, 'How does China censor the Internet?' (Version: 21 April 2013) http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-china-censors-internet (27 December 2015).
[93] Walton, *China's golden shield*, 5.
[94] L. M. Hinman, 'Esse est indicato in Google: Ethical and Political Issues in Search Engines', *International review of information ethics* 3 (2005) 20-25, 24.
[95] C. Hatton, 'China 'Social Credit''.
[96] Reuters 'Ant Financial Unveils China's First Credit-Scoring System Using Online Data' (Version: 27 January 2015) http://www.reuters.com/article/ant-financial-services-idUSnBw276582a+100+BSW20150128 (26 December 2015).

China. Under the draft counter-terrorism law published in 2014, the Chinese government demands that "Telecommunications operators and Internet service providers shall install technical interfaces in the design, construction and operations of telecommunications and the Internet, and report cryptography schemes to departments responsible for encryption for examination."[97] This basically means that private operators who want access to the Chinese market are required to incorporate ways for the Chinese authorities to intercept data streams, enabling mass-surveillance.[98] According to Yuan Chang, a Chinese blogger, Chinese authorities are already engaging in mass-surveillance. In a speech on an online influencers platform in the Netherlands he stated: "In China there is no such thing as privacy: [The government] knows everything about you".[99]

Manual content editing and monitoring

The online surveillance is taking place on many levels. At the turn of the last century the MPS was controlling regional centres for Internet security, that created lists of URLs that could be blocked locally by a predetermined filter when users tries to access it at the local level.[100] Next to this filtering mechanism, there was also physical control as people were hired to perform routine checks in Internet cafes. A *Human Rights Watch* report states that in 2001 it was common practice that Internet Café were patrolled by people that were checking monitors for forbidden materials.[101]

Around the same time Internet forums and discussion boards, known as Bulletin Board Systems (BBS), became popular mediums for Chinese people to interact on the Internet. To regulate the content on BBSs regular Internet users were picked to volunteer as forum managers.[102] Today people are still hired to manage the content on websites and forums and the practice of manual content regulation remains an important ingredient for the control of content on the Internet by Chinese authorities.[103]

While most online editors are in direct service of the online platforms they work for, the Chinese government reportedly has around two million people employed to police online public opinion.[104] One of such government employees, Tang Xiaotao, told the Bejing News that his daily job

---

[97] China Law Translate "Counter-Terrorism Law (initial draft)" (Version: 08 November 2014) http://chinalawtranslate.com/ctldraft/?lang=en (26 December 2015).
[98] T. H. Moran, 'Cyber surveillance regulations: Is the United States asking China to accept a double standard?', *American Enterprise Institute* (20 April 2015) https://www.aei.org/publication/cyber-surveillance-regulations-is-the-united-states-asking-china-to-accept-a-double-standard/ (29 Decmeber 2015).
[99] RNW Media, "Bloggers Open Borders for the Media" (Version: 14 January 2016) https://www.rnw.org/articles/bloggers-open-borders-for-the-media (22 January 2016).
[100] Walton, *China's golden shield*, (page no. unkown).
[101] 'Freedom of expression and the Internet in China', *Human Rights Watch*, 5.
[102] G. Yang, 'Internet Activism & the Party-State in China', *Daedalus* 143 (2014), 110-123, 115.
[103] Yang, 'Internet Activism & the Party-State in China', 115.
[104] T. Lum, "Human Rights in China and U.S. Policy: Issues for the 114th Congress", *Congressional Research Service* (Version: 24-03-2015) https://www.hsdl.org/?view&did=765959 (09-03-2016).

is to use advanced software applications to filter through Internet messages, searching for keywords on which to base his reports.[105]

Propaganda Campaigns

A central feature of Chinese Internet regulation is the targeting of Internet users with large-scale propaganda campaigns. These campaigns were outlined in the 2010 White Paper on the Internet in China, in which they fall under the category of "social education" of the crowds.[106] One of the propaganda campaigns exists of people posting favourable online content on social media platforms, defending the Chinese government against online criticism. It is estimated that there are between ten thousands and hundred thousands of these online commentators that try to steer online discussion, by commenting directly on people who express their discontent with the Chinese government.[107] The existence of these commentators is widely known by Chinese Internet users, who have dubbed them Wumao – Mandarin for fifty cents - referring to them being paid by the government for every successful online post.[108]

According to Guobin Yang, expert on the Chinese Internet, these propaganda campaigns show that the Chinese government has recently taken on a new approach to Internet regulation that focuses on soft power. He explains that back in the early 2000's the government often took very restrictive measures on an ad hoc basis to control Internet content, but that lately more emphasis is placed on exerting "soft control".[109] He gives an example of this soft control by quoting a local study of the Fujian province on Internet regulation on municipality level. One of the best practices was that of the municipal public security bureau of Jian'ou. The bureau located people posting harmful content and explained the negative effects of their posts in order for them to voluntarily remove their own content.[110]

The Internet as a buffer zone

Despite the firm grip of the Chinese authorities on the Internet, it is still an important place for citizens to voice their opinion and even to organize protests. According to Yang the Internet played an important part in the online mobilization of people for offline protests in China and writes that

---

[105] K. Hunt and C. Xu, 'China 'Employs 2 Million to Police the Internet'', *CNN* (version: 7 October 2013) http://edition.cnn.com/2013/10/07/world/asia/china-internet-monitors/ (2 January 2016).
[106] Information Office of the State Council of the People's Republic of China, 'White paper (IV)'.
[107] D. Wertime, 'How to Spot a State-Funded Chinese Internet Troll', *Foreign Policy* (Version; 17 June 2015) http://foreignpolicy.com/2015/06/17/how-to-spot-a-state-funded-chinese-internet-troll/ (02 January 2016).
[108] Wertime, 'How to Spot a State-Funded Chinese Internet Troll'.
[109] Yang, 'Internet Activism & the Party-State in China', 116.
[110] Ibidem, 116.

"internet activism is one of the most important forms of citizen activism in China."[111] Indeed, despite all efforts of the Chinese government to regulate web-based content, there are multiple examples of citizens criticizing government officials online. In some cases this has led to the prosecution of government officials that were online accused of being corrupt. [112]

However, most of this online social unrest is targeting specific government officials and is not threatening the communist party leadership as a whole. Zixue Tai believes that the Chinese government uses the online environment as a "buffer zone" in which they can get a sense of public sentiment before it grows to big.[113] It would even be possible that the Chinese government sacrifices some low level government officials to make the Chinese people feel they have a say, while at the same time distracting them from protesting against bigger issues of government control.

While the Chinese authorities have found effective ways to censor online content, Chinese citizens come up with ingenious ways to pass government filtering. In order to do so, they make use of audio-fragments, videos, images, metaphors and puns in which they criticize the government.[114] Electronic filter systems have a hard time picking up these posts, as they don't contain prohibited keywords. One widely known example of civil disobedience on the Internet is *Căonímă,* which translates to 'grass mud horse' and sounds like a Chinese profanity. As government set Internet filters couldn't filter Căonímă the term became a symbol of defiance of online government repression.[115] This type of social protest, however, is often scattered and mostly satirical in nature and therefore seems relatively harmless to the Chinese institutions.

Summary

All in all the Chinese government has set up a complex control mechanism for the Internet in which hard power is combined with soft power to regulate the behaviour of Chinese citizens on the Internet. The Chinese government has implemented an extensive body of legislation, which allows the authorities to hold both citizens and organisations accountable for online content that can be linked to them. Legal prosecution, loss of licences, URL-blocks, manual editing and monitoring, and self-censorship enforce compliance to the rules set by the Chinese government. These measures are complemented by the exertion of soft power through propaganda the use of the Internet as a buffer zone for public opinion.

---

111 Yang, 'Internet Activism & the Party-State in China', 110-111.
112 Z. Tai, 'Networked Resistance: Digital Populism, Online activism, and mass dissent in China', *Popular* communication, 13 (2015), 120-131, 128.
113 Tai, 'Networked Resistance', 130.
114 Freedom House, 'Freedom on the Net 2015: China', *Freedom House* (version: 2015) https://freedomhouse.org/sites/default/files/resources/FOTN%202015_China.pdf (03 December 2016), 14.
115 X. Chiang, 'The Battle for the Chinese Internet', *Journal of Democracy* 22 (2011) 47-60, 52.

The Chinese authorities have gone through great lengths to regulate the domestic Internet, leaving little to no room for citizens and organisations to circumvent government control and to express anti-government sentiment on the Internet. Over the years the Chinese government has recognized the potential of the Internet to strengthen it's control over Chinese citizens by using it to explore mass-surveillance techniques. Most recently they have started to pilot a new technique to rate Chinese citizens based on their Internet behaviour. I therefore conclude that since 1994 the Internet has showed no signs of posing serious threats against Chinese domestic sovereignty. If anything, Chinese authorities have mastered the Internet and are capable of using it to spread propaganda, improve governmental structures and increase surveillance, resulting in enhanced state control.

3.2 The influence of the Internet on China's interdependence sovereignty

When China was linked to the global Internet in 1994, the Chinese government soon realised that there would be previously unseen amounts of interconnectivity between China and the rest of the world. Realizing the consequences of free flows of information on the authoritarian system, the aim was not just to control the domestic cyber domain but also to control China's Internet connections to the outside world.[116] What measures did the Chinese government take to defend its interdependence sovereignty? And how successful has China been so far in controlling the influx of information flows from abroad?

The Great Firewall of China

In the late 1990s the Chinese authorities designed a system that would lead all international Internet traffic and data streams through funnels, better known as "gateways", when entering the Chinese domestic web environment.[117] This construction lies at the base of what later became known as the Great Firewall of China and was designed to be able to control citizens' access to forbidden websites and censored information from abroad.[118] The firewall was refined in May 2000 by incorporating a state of the art filtering systems, known as the 'National Information Security Management System'. According to *The Economist* this system, designed by Fang Binxing, has been "the most critical and most expensive component" in constructing the Great Chinese Firewall.[119]

Nowadays these gateways are still the main entrance point of foreign Internet traffic to China, enabling the government to heavily restrict international data transfer. According to Svensson "[t]his

---

[116] Walton, *China's golden shield,* 9.
[117] Walton, *China's golden shield,* 9.
[118] Tsui, 'The Panopticon as the Antithesis of a Space of Freedom', 68.
[119] The Economist, 'The great Firewall: The Art of Concealment', (Version: 6 April 2013) http://www.economist.com/news/special-report/21574631-chinese-screening-online-material-abroad-becoming-ever-more-sophisticated (05 January 2016).

involves IP blocking, DNS tampering, filtering of sensitive words and topics, leading to the blocking of International websites such as that of *The New York Times* and human rights organizations."[120] Since the erection of the firewall, the system has continuously been improved. While at first it was blocking entire lists of URLs, the system now searches for keywords and only blocks certain forbidden pages within websites, making it the most advanced national firewall in the world.[121] The blueprint of the Great Firewall is a Chinese state secret, but many scientists and hackers have tried to unravel its mysteries, making it possible to provide a general overview of the way it operates. The regulation of online trans-border flows is maintained by an ingenious structure embedded in multiple layers of the Internet.

The Ministry of Information Industry and Technology (MIIT) is the architect of the Chinese firewall and keeps general oversight of the cross-border information flows.[122] It has constructed three Chinese state-run Internet Exchange Points (IXPs) through which all ingoing and outgoing Internet traffic passes. These IXPs are peered by state-licensed Internet Access Providers (IAPs) whom all have at least one connection to a prominent international data route, called an Internet backbone. The IAPs provide global network access to local Internet service providers (ISPs) whom in their turn provide end-users with access to the World Wide Web. The Chinese ISPs can be seen as "retail sellers" of Internet access to the end-user.[123] Four state-controlled companies operate both the IXPs and IAPs, handing the Chinese state the ultimate control of all incoming and outgoing data.[124]

All Chinese networks are connected through routers that guide the Internet traffic through the Internet and to the right server. These routers are actual devices that are situated at cross-sections of networks. This means that there are routers situated between the ISP and the IAP and between the IAP and the backbone it connects to. Routers allow for network administrators to filter data that passes through them. They are equipped with technology that can filter for keywords in order to block any type of unwanted content. In the case of China both ISP and IAP routers are programmed to filter on forbidden URLs and keywords. This means that content is filtered both in the "lower layer" and the "upper layer" of the Chinese Internet.[125]

According to a *Human Rights Watch* report, the decision of what content should be censored by these filters is made by the Communist Party's Propaganda Department on advice of government and public security organs.[126] In the end it is their decision to block websites like Facebook and BBC

---

120 Svensson, "Internet in China and its Challenges for Europe', 4.
121 The Economist, 'The great Firewall: The Art of Concealment'
122 Freedom House, 'Freedom on the Net 2015: China', 4.
123 Human Rights Watch, 'How Censorship Works in China: A Brief Overview' (Version: August 2006) https://www.hrw.org/reports/2006/china0806/3.htm (03 January 2016).
124 J. Lee and C. Liu, 'Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China', *Minnesota Journal of Law, Science, and Technology* 14 (2012), 125-151, 134.
125 Lee and Liu, 'Forbidden City Enclosed by the Great Firewall', 135.
126 Human Rights Watch, 'How Censorship Works in China'.

and to webpages that feature words like "Tibetan independence" and "human rights".[127] According to the American based human rights organisation *Freedom House,* tens of thousands of websites are blocked by the IAPs, with one of the latest developments being the complete block of Google's website and services.[128]

The Chinese approach of website blocking and content filtering is not a 'one size fits all' solution. Jyh-an Ly and Ching-Yi Liu write that the amount of control that the Chinese authorities have over Chinese cyberspace would not have been possible if they hadn't dominated the design and construction of the Chinese cyber domain from the very start. They argue that China's architecture of the Internet is profoundly different from that of the Internet in the Western world, where it is much more open and decentralized and therefore harder to regulate.[129]

Fighting anonymity on the web

While the Great Firewall heavily restricts the access of Chinese citizens to foreign information, there are ways to circumvent the measures taken by the Chinese authorities in order to access forbidden websites. The most common way is the use of Virtual Privat Networks (VPNs). When using a VPN a computer takes on the IP-address of the VPN, tricking ISPs content filters to believe it is located somewhere else. In the early 2000s, the Chinese Academy of Social Sciences conducted a survey that showed that at least ten per cent of the Internet users in China regularly used a proxy server to circumvent censorship.[130]

However, most VPNs in China are slow and unstable and to be able to use them you need some extent of technical knowledge.[131] The Chinese government never paid much attention to blocking VPNs until an online attack in 2015 that disrupted the three largest providers of VPN services. The Chinese government later acknowledged responsibility, claiming that the attack was part of an upgrade of the Great Firewall of China.[132] Although the access to the VPNs has been restored since, it shows the lengths through which Xi will go to regulate the Internet. It is, however, unlikely that he will shut down all VPNs as this will eventually harm international business. To support the economy he will need to leave the door to the Internet of the rest of the world ajar, resulting in some extent of "Collateral Freedom" on the Internet.[133]

---

[127] Open Net Initiative, 'China profile', (Version: 09 August 2012) https://opennet.net/research/profiles/china-including-hong-kong287 (05 January 2016).
[128] 'Freedom on the Net 2015: China', *Freedom House,* 2.
[129] Lee and Liu, 'Forbidden City Enclosed by the Great Firewall', 142.
[129] Human Rights Watch, 'How Censorship Works in China'.
[130] Walton, *China's golden shield,* (page no. unkown).
[131] Svensson, "Internet in China and its Challenges for Europe', 5.
[132] S. Yuen, 'Becoming a Cyber Power: China's Cyber Security Upgrade and its Consequences', *China perspectives* 2 (2015) 53-58, 53.
[133] Svensson, "Internet in China and its Challenges for Europe', 5.

Apart from VPNs, Chinese citizens make use of proxy servers and TOR. TOR is software that creates a random path through cyberspace, making several stops on different servers before reaching it destination. When it makes a stop on a server it forgets the previous destination, making it impossible to link back the data flow to its origins. According to a *Human Rights Watch* Report from 2006, tens of thousands of Chinese citizens were making use of TOR on a weekly basis. The report states that they lack an explanation for the reason that China has not been blocking proxy nodes used by TOR.[134] However, a more recent article in *The New York Times* revealed that the authorities have found a way to discourage the use of TOR. Reportedly, Chinese hackers succeeded in finding users of TOR by comparing the IP-address of people who were accessing compromised websites with IP-adresses of people who were logged on to one of the fifteen major Chinese Internet portals.[135] The result is that even use of this deeper layer of the Internet is no longer a safeguard of anonymity for Chinese Internet users.

Summary

The Chinese firewall is a very well designed and sophisticated structure and comes as close to a virtual border of cyber territory as it gets. It enables the Chinese government to filter and censor any information flows that are perceived as harmful to the regime. One of the reasons that the Great Firewall of China proves to be so effective, is that the Chinese authorities have been involved in the architecture of the domestic cyber domain from the very start. Although there are some tools to circumvent government control on the Internet, the use of these tools is far from ideal, as they can be slow, require some extent of technical knowledge, and, lately, have been compromised by hackers.

The Chinese government has secured its cyber territory by building a large cyber wall, shielding of the Chinese citizens of the unwanted international data streams that carry liberal ideas and political threats. Despite the ability of some tech-savvy citizens that can circumvent this control, the effect of the Internet on interdependence sovereignty of China can therefore be judged to have had a negligible effect.

3.3 The influence of the Internet on China's Westphalian sovereignty

According to the Westphalian principle all states have the right to non-intervention in their national affairs. Although this convention is widely accepted and forms the foundation of contemporary international affairs, it does not reach into the cyber domain. The set-up of the Internet finds it origins in Western values and is governed by a multi-stakeholder model, leading to the discontent of

---

[134] Human Rights Watch, 'How Censorship Works in China'.
[135] N. Pelroth, 'Chinese Hackers Circumvent Popular Web Privacy Tools', *The New York Times*, 12 June 2015.

authoritarian states, which need to share their power over the Internet with other stakeholders.[136] The past years China has led an extensive lobbying campaign to push for Westphalian sovereignty on the Internet. During the Global Internet Conference 2015 president Xi emphasised the importance of sovereignty in cyberspace and the need for "respecting each country's right to choose its own internet development path, its own internet management model, its own public policies on the internet […] avoiding cyber-hegemony, and avoiding interference in the internal affairs of other countries."[137]

Apart from securing its Westphalian sovereignty from the leverage of foreign actors Xi also recognized the importance of securing the Chinese Internet from the coercion or infiltration of foreign powers by stating: "without network security there is no national security."[138] What measures does the Chinese government take to defend its Westphalian sovereignty? To what extent is China able to secure its Westphalian sovereignty against Western dominance in Internet governance?

A multilateral model of the Internet

Since the construction of the Internet its technical governance is conducted through a multi-stakeholder model in which power is divided between governments, private corporations and civil society. Already since the late 1990s the Chinese government has tried to change the way the Internet is globally governed towards a more multilateral model, leaving the highest decision-making authority at the state level.[139] By doing so, it wants to regain its authority to regulate the Internet within Chinese territory without any type of foreign intervention.[140]

One of the most important organisations in the governance of the Internet is the Internet Corporation for Assigned Names and Numbers (ICANN). The organisation provides a global administration of the Internet, making sure that there is just one authority for domain names and IP-addresses to avoid fracturing of the Internet.[141] This means that all countries that participate in ICANN are voluntarily trading a part of their Westphalian sovereignty, which allows them to create their own Internet legislation, for the benefits of a globally organized Internet structure.

---

[136] T. Galloway and H. Baogang, 'China and Technichal Global Internet Governance: Beijing's Approach to Multi-Stakeholder Governance within ICANN, WSIS and the IGF', *China: An International Journal* 12 (2014) 72-93 ,79.
[137] D. Bandurski 'China's Cyber-Diplomacy', *China Media Project* (Version: 21 December 2015) http://cmp.hku.hk/2015/12/21/39527/ (06 January 2016).
[138] J. McReynolds, 'China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy' *The Jamestown Foundation* (Version:16 April 2016) http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=43798&no_cache=1#.VrG5uXgmf3c (02 Februari 2016).
[139] Galloway and Baogang, 'China and Technichal Global Internet Governance', 72.
[140] M. Jiang, 'Authoritarian Informationalism: China's approach to the Internet', *SAIS Review* 30 (2010) 71-89, 73.
[141] Galloway and Baogang, 'China and Technichal Global Internet Governance', 79.

However, ICANN is an American Based Non-Profit organisation, in which the U.S. has the largest share of power.[142] Both the multi-stakeholder model and the U.S. hegemony within ICANN has resented China and led to the country non-participation in ICANN from 2001 to 2009. In the end the Chinese government realized that it was unfeasible to not be part of ICANN, as a separate Chinese network or Intranet would greatly damage its technical and economical interests and joined ICANN again.[143]

In the meantime China has been lobbying for a more multilateral approach to the Internet, with the back up of other authoritarian countries, like Russia, Algeria, Iran and Saudi Arabia.[144] Recently, China's lobby has started to pay off. A 2015 UN document that was set to define policies for future Internet governance include: "a leading role for governments in cyber security matters". Later Chinese negotiators commented that the outcome of the document was in China's interest.[145] In a speech on the second World Internet Conference in 2015, Xi denounced the U.S. monopoly on cyber governance.[146] He stated that with the largest share of Internet users, China should have a say in the regulation of the global Internet.[147] Until a more multilateral approach is taken, however, the Chinese government will have to come to terms with some loss of Westphalian sovereignty as multiple parties have a say on how the Internet is to be structured.

Countering cyber threats, cyber espionage and ideological warfare

While the Chinese have always put great effort in controlling their networks and securing their domestic and interdependence sovereignty, they have only recently publicly announced that they are building a military cyber force to protect China from foreign cyber power to secure their Westphalian sovereignty against external threats in the cyber domain. Every 15 years the Chinese People's Liberation Army's Academy of Military science publishes a study called the Science of Military Strategy (SMS) which describes the army's strategic course.[148] In 2013 a new edition of the SMS was published, which revealed that China has build up a cyber force that is capable of attack.

According to the document the Chinese have created three types of cyber attack forces: Specialized military network operational units, teams of authorized network warfare specialists who work in public agencies, and non-governmental forces that can be engaged in network attacks or

---

142 Galloway and Baogang, 'China and Technichal Global Internet Governance', 79.
143 Ibidem, 82.
144 K. Maher, 'The New Westphalian Web', *Foreign Policy* (Version: 25 February 2013) http://foreignpolicy.com/2013/02/25/the-new-westphalian-web/ (06 January 2016).
145 D. Levin, 'At U.N., China Tries to Influence Fight Over Internet Control', *The New York Times,* 16 December 2015.
146 S. Tiezzi, 'China vows no compromise on cyber soveregnty', *The Diplomat* (Version 16 December 2015) http://thediplomat.com/2015/12/china-vows-no-compromise-on-cyber-sovereignty/ (06 January 2016)
147BBC News, 'China internet: Xi Jinping calls for cyber sovereignty', (Version: 16 December 2015) http://www.bbc.com/news/world-asia-china-35109453 (06-01-2016).
148McReynolds, 'China's Evolving Perspectives on Network Warfare'.

defence on an ad hoc basis.[149] In the document the importance of the role of the IT-industry is stressed, as this is the breeding ground of IT specialists and an important resource for technical expertise that lies at the foundation of the Chinese cyber force.[150] The document also reveals that one of the key components of Chinese network strategy is peacetime "network reconnaissance", which is reached by the penetration and continuous monitoring of adversaries' networks. The ultimate aim is to be able to transform this 'peaceful' presence on foreign networks into active disruption when under pressure.[151]

While the actual establishment of a cyber force has never been officially acknowledged before 2013, the Chinese government has been engaged in cyber security initiatives since 1986. Even before China was connected to the Internet, the establishment of State Economic Information Management Leading Small Group, was the first step towards exploring information structures and their relation with national security.[152] Later on China established the State Network and Information Security Coordination Group in 2003, which also focussed on the network vulnerabilities to cyber threats from outside.[153] Amy Chang, research fellow at the Centre for a New American Security, an American Research Centre that conducts fact-based research on U.S. security debates, writes that "Despite China's on-going efforts to coordinate and organize the network security infrastructure, it remains fragmented."[154]

It was president Xi who has tried to bring together all cyber initiatives under a comprehensive strategy for cyber security.[155] In 2015 the Ministry of defence published a White Paper on its military strategy. The White paper acknowledges the serious security threats that are imposed on China by the "informatization" of society and discusses the necessity to establish Chinese offensive cyber capabilities in order to maintain China's overall military strategy of active defence.[156] Although the White Paper is a document that describes China's military strategy in all domains, the cyber domain is identified as a critical component of national security:

> As cyberspace weighs more in military security, China will expedite the development of a cyber force, and enhance its capabilities of cyberspace situation awareness, cyber defense, support for the country's endeavors in cyberspace and participation in international cyber cooperation, so as

---

[149] McReynolds, 'China's Evolving Perspectives on Network Warfare'.
[150] Ibidem.
[151] McReynolds, 'China's Evolving Perspectives on Network Warfare'.
[152] A. Chang, 'Warring State: China's Cybersecurity Strategy', *Center for a new American Security* (Version: December 2014) http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang_report_010615.pdf (3 February 2016), 16.
[153] Chang, 'Warring State', 16.
[154] Ibidem, 10.
[155] Ibidem, 9.
[156] Chinese People's Liberation Army 'China's Military Strategy', (Version: 26 May 2015) http://english.chinamil.com.cn/news-channels/2015-05/26/content_6507716_6.htm (3 February 2016).

> to stem major cyber crises, ensure national network and information security, and maintain national security and social stability.[157]

While the Chinese government is increasingly securing the nation against foreign cyber attacks and espionage, the main focus of the Chinese military remains to uphold the authority of the Communist Party. As the above fragment of the White Paper describes an important component of maintaining national security is to ensure "social stability".[158] The document literally states: "China's armed forces always treat ideological and political building as the first priority, and have endeavored to reinforce and improve their political work in the new situation."[159]

Summary

When it comes to China's Westphalian sovereignty it is being threatened in two ways. The first is what Krasner calls erosion of Westphalian sovereignty "by invitation". The Chinese government is trading a little of its Westphalian sovereignty against a seat in ICANN. It does so voluntarily as it is not coerced into doing so by force. It is, however, putting great effort into reforming the principles on which the Internet is governed and is supported by other authoritarian countries in doing so.

The second threat is the erosion of Westphalian sovereignty "by infiltration", meaning by force. Although the Chinese government has recognized the potential security threat of the Internet, its cyber security measures have been scattered amongst its many government organisations. Under leadership of Xi more emphasis has been placed on securing China against cyber threat, cyber espionage and ideological warfare on the Internet.

Both the SMS and the White Paper on Chinese military strategy show that the cyber domain is treated as an operational domain that must be secured against foreign adversaries. While the threats of cyber attacks and cyber espionage are real, the main focus of the Chinese military lies at securing the nation of ideological penetration. The biggest concern of the Chinese government is that foreign powers will use the Internet to spread sensitive information that could lead to the loss of authority or legitimacy of the Communist Party, resulting in a loss of Westphalian sovereignty.

4. The U.S. and the rise of the Internet

One of the primary goals of U.S. foreign policy is to promote Internet access and freedom. The U.S. Office of International Communications and Information Policy writes on its website that its aim is to achieve access to the global Internet for any child "as an open platform on which to innovate, learn,

[157] Chinese People's Liberation Army 'China's Military Strategy'.
[158] Ibidem.
[159] Ibidem.

organize, and express herself free from undue interference or censorship".[160] As part of this U.S. policy the authorities promote unlimited access to websites across the globe and fight censorship on the web. This policy is diametrically opposed to Chinese Internet policy that heavily restrains the interconnectivity of its citizens and places great emphasis on censorship. It seems however, that even the U.S. is not immune to regulating the Internet to at least some extent. Although the U.S. is still in the top ten of the 'Freedom on the Net' report of *Freedom House*, its position has been slowly falling down the rank as its Internet has become both in relative and absolute terms less free than previous years.[161]

The U.S. has had a huge influence on the design of the infrastructure and the regulation of the global Internet. The Internet was invented in the U.S. as a military communication system and was later used as a blue print for scientists to link university networks. The Internet was shaped to facilitate the free flow of information and its academic origin supported a non-hierarchical structure: values that were in line with the liberalist- and individualistic nature of the U.S..[162] The past years, however, it appears that there are certain downsides to these liberal values on the Internet. Apart from a medium for the spread of democratic values, the Internet has proven to harbour terrorist networks and disseminate sensitive or even classified government information.[163] Being a liberal democracy with strong morals and many foreign enemies, the U.S. has to constantly weigh its liberal values against security considerations when shaping Internet policy.

To what extent is the U.S. able to maintain its domestic-, interdependence- and Westphalian sovereignty in cyberspace? In this chapter I will analyse the influence of the Internet on U.S. state sovereignty by applying Krasner's framework on sovereignty to U.S.' policies and regulation of the Internet. Keeping in mind that the Internet policies and regulations of the U.S. are profoundly different from those of China, it will be interesting to examine both countries' approaches to securing state sovereignty in the age of the Internet and to compare their effectiveness.

4.1 The influence of the Internet on U.S.' domestic sovereignty

The U.S.' Internet is classified as free and the U.S. is one of the freest countries when rated on obstacles to access, limits on content and violations of user rights on the Internet.[164] This is in line with

---

[160] U.S. Department of State, 'Internet Freedom', http://www.state.gov/e/eb/cip/netfreedom/index.htm (09 January 2016).
[161] Freedom House, 'Freedom on the Net 2015' (Version: 2015) https://freedomhouse.org/report/freedom-net/freedom-net-2015 (10 January 2016).
[162] J. C. Rodriguez, "Comparative Study of Internet Content Regulations in the United States and Singapore: The Invincibility of Cyberporn, A." *APLPJ* (Version: 2000) http://cyber.law.harvard.edu/ilaw/Speech/Rodrig.htm, (12 January 2016).
[163] The White House 'International Strategy for Cyberspace', (Version: may 2011) https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (13-01-2016), 5.
[164] Freedom House, 'Freedom on the Net 2015'.

the liberal Western values that the U.S. stands for, but it also provides relatively little government control over what its citizens do in the cyber domain. Recently it became clear however, that this Internet freedom comes with a price tag. In 2013 Edward Snowden leaked secret documents that revealed that the U.S. authorities are constantly monitoring and analysing its citizens Internet data through large-scale surveillance operations conducted by the NSA.[165] Despite the Internet freedom, the U.S authorities have found ways to establish mechanisms of control in the U.S. cyber domain. How does the U.S. secure its domestic control in the cyber domain? And to what extent is it successful in regulating the U.S. citizens in cyberspace?

Law and cyber legislation

The right to freedom of speech is guaranteed to U.S. citizens by the First Amendment and is firmly rooted in the U.S. system of law. In 1997 the U.S. Supreme Court decided in a court case that Internet speech is entitled to the highest level of First Amendment protection.[166] Removing or censoring online content would therefore in most cases be in conflict with the American constitution. The U.S. has no track record of prosecuting individuals for online speech and lower courts have consistently decided against attempts to regulate online content.[167]

Even though the U.S. is barely restricting online content, this does not mean that the state authorities have no control over what happens within the U.S. cyber domain. Betz and Steven write:

> There are many […] examples that could be used to illustrate how both liberal and authoritarian governments are pursuing forms of control over cyberspace in order to mitigate perceived threats against domestic sovereignty. In the West and elsewhere, terrorism is commonly invoked as the justification for doing so.[168]

The same goes for the U.S. government, which has been accused of executing large-scale surveillance operations targeting ordinary U.S. citizens in the aftermath of 9/11.[169]

There are multiple laws that provide state authorities with the right to obtain records of its citizens. One of the most controversial pieces of legislation is the Patriot Act. The act was passed in congress on 26th of October 2001, right after the 9/11 attacks, and facilitates the collection of

---

165 C. Arthur, 'NSA scandal: what data is being monitored and how does it work?' *The Guardian*, 7 June 2013.
166 D. L. Hudson, 'Hate Speech Online' *First Amendment Center* (version: 13 December 2002) http://www.firstamendmentcenter.org/hate-speech-online (12 January 2015)
167 Freedom House 'Freedom on the net 2014: United States', (Version: 2014) https://freedomhouse.org/sites/default/files/resources/United%20States.pdf (12 January 2016).
168 Betz & Stevens, *Cyberspace and the State,* 68.
169 American Civil Rights Union, 'Testimony of Jameel Jaffer and Laura W. Murphy before the Senate Judiciary Committee', (Version: 31 July 2013) http://nsarchive.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-111e.pdf (12-01-2016).

communication records. The act would later form the basis for the NSA to monitor and track the communication of American citizens.[170] There has been a lot of controversy about the Patriot Act, because there is a lack of control on the way the search warrants are obtained. Theodore Moran, professor in public policy at the Georgetown University, writes: "Neither the FBI nor NSA needs to show probable cause or even reasonable grounds to believe that the person whose records it seeks is engaged in criminal activity […]the only limitation in the Patriot Act is that the secret warrant has to be "relevant" to a national security investigation."[171]

Another law that seems to be threatening the privacy of ordinary citizens is the Electronic Communications Private Act (ECPA). The law that was passed in 1986 gives executive agencies the power to obtain private records of people directly from service providers without an official warrant.[172] Because some of the information that service providers are asked to disclose can be of very sensitive nature, the original ECPA had a provision that stated that records could only be obtained "if [the FBI] could certify that (i) the information sought was relevant to an authorized foreign counterintelligence investigation; and (ii) there were specific and articulable facts giving reason to believe that the subject of the NSL was a foreign power or foreign agent."[173] In 2001 Congress adopted revision of the act that according to the *U.S. Civil Rights Union* meant that the prerequisits for the use of ECPA were significantly loosened, leading to the exponential growth of warrants.[174]

In 2011 a new cyber security bill was introduced in the Senate called CISPA. The bill would allow companies to share data with the government, without any type of court order. *Reporters without borders* called CISPA a way to "deploy draconian measures to monitor, even censor, the Web."[175] In the end the bill didn't pass, but four years later the senate passed a similar bill, called the Cybersecurity Information Sharing Act (CISA). Stakeholders and human rights advocates believe that the act might lead to the invasion of citizens' privacy and provides the U.S. government with a new means for large-scale government surveillance programs.[176] The Computer and Communications Association (CCIA), with members like Facebook and Google, has published an open letter to congress, warning that "CISA's prescribed mechanism for sharing of cyber threat information does not sufficiently protect users' privacy or appropriately limit the permissible uses of information shared

---

[170]American Civil Rights Union, 'Testimony of Jameel Jaffer and Laura W. Murphy'.
[171]American Enterprise Institute, "Cyber surveillance regulations: Is the United States asking China to accept a double standard?", (Version: April 2015) https://www.aei.org/wp-content/uploads/2015/04/Cyber-surveillance-regulations.pdf (12 January 2016).
[172]Freedom House 'Freedom on the net 2014'.
[173]American Civil Rights Union, 'Testimony of Jameel Jaffer and Laura W. Murphy'.
[174]Ibidem.
[175]Reporters Without Borders, 'Draconian Cyber Security Bill Could Lead to Internet Surveillance and Censorship', (version: 04 June 2012) http://en.rsf.org/etats-unis-draconian-cyber-security-bill-06-04-2012,42283.html (03-02-2016).
[176]D. E. Sanger and N. Perlroth 'Senate Approves a Cybersecurity Bill Long in the Works and Largely Dated', *The New York Times*, 27 October 2015.

with the government."[177] Despite the Snowden revelations, the U.S. authorities seem to have acquired more control over domestic information flows the past years.

In addition to the above acts that provide the U.S. authorities with legal grounds to issue warrants for obtaining data, there is also legislation that allows the U.S. government to directly collect data at the source. The Communications Assistance for Law Enforcement Act (CALEA) obliges all telecommunications carriers to build in backdoors into their equipment and software and to turn over encryption keys.[178] One of the organisations that comply with CALEA is Cisco, who provides routers that connect service providers to the backbone of the U.S. Internet and can thus directly be tapped by the U.S. authorities.[179] A leaked power point presentation from the NSA head quarters confirms that the NSA also obtained direct access to Google, Apple and other service providers. The NSA allegedly had access to e-mails, search histories and file transfers.[180]

Large-scale monitoring and surveillance

One of the problems with the above laws is that there is a lack of transparency and oversight in data collection practices of the U.S. intelligence agencies and therefore a lack of accountability to the general public. Already in 2011 the *Electronic Frontier Foundation* (EFF), a digital rights organisation, detected an "alarming trend" of unlawful Internet Surveillance by the Federal Bureau of Investigation (FBI) between 2001 and 2008. According to the *EFF* there was insufficient oversight and accountability.[181]

Three years later Edward Snowden expressed the same fears as he addressed his concerns over the lack of institutional oversight and accountability regarding NSA surveillance practices in an interview with two journalists of the Guardian.[182] According to Snowden the data collection practices far outreached the initial goal of state security. In the interview he states:

> The government assumed upon itself, in secret, new executive powers without any public awareness or any public consent and used them against the citizenry of its own country to increase its own power, to

---

[177]B. Madhani "CCIA Urges Senate To Improve Cybersecurity Information Sharing Act" *Computer & Communications Industry Association* (Version: 15 October 2015) http://www.ccianet.org/2015/10/ccia-urges-senate-to-improve-cybersecurity-information-sharing-act/ (13 January 2016).
[178]T. H. Moran, 'Cyber surveillance regulations: Is the United States asking China to accept a double standard?', *American Enterprise Institute* (Version: 20 April 2015) https://www.aei.org/publication/cyber-surveillance-regulations-is-the-united-states-asking-china-to-accept-a-double-standard/ (29 December 2015).
[179]Arthur, 'NSA scandal'.
[180]Greenwald and MacAskill, 'NSA'.
[181]The Electronic Frontier Foundation, "Patterns of Misconduct: FBI Intelligence Violations from 2001 – 2008" (version: 23 January 2011) https://www.eff.org/wp/patterns-misconduct-fbi-intelligence-violations#8 (15 January 2016).
[182] A. Rusbridger and E. MacAskill, 'Edward Snowden Interview – the edited transcript', *The Guardian,* 18 July 2014.

> increase its own awareness […] What I came to feel […] is that a regime that is described as a national security agency has stopped representing the public interest and has instead begun to protect and promote state security interests.[183]

Snowden points out that the surveillance practices of the NSA are ultimately a means of the U.S. authorities to consolidate their own power.

This vision is in line with a report on Internet governance by the Commissioner for Human Rights at the Council of Europe. In an issue paper for the council of Europe the paper comments the following: "it is becoming increasingly clear that secret, massive and indiscriminate surveillance programmes are not in conformity with European human rights law and cannot be justified by the fight against terrorism or other important threats to national security."[184] In this matter the independent report of the Commissioner of Human Rights agrees with Snowden that national security is not a legitimate basis for large scale Internet surveillance.

One of the programs of the NSA that raised concerns is the PRISM program, which enabled the NSA to bulk collect data straight from the servers of Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple. Amongst the collected data are emails, audio- and video chats, and photographs.[185] The exact extent of the program is shredded in secrecy as all major service providers denied any knowledge of PRISM.[186] *The New York Times* reported on the construction of a "one-million-square foot fortress in the mountains of Utah, apparently to store huge volumes of personal data indefinitely."[187] With the diminishing costs of data storage, the permanent storage of data is becoming increasingly attractive.

While the lion's share of people will probably not notice the intrusive surveillance programs on the Internet, there are some groups of people that indicate that they experience discomfort while communicating via the Internet in the U.S.. In a survey conducted by *Human Rights Watch*, journalists indicated that the large-scale surveillance programs of the NSA has compromised their confidential communication, feeling the need to take measures to secure information lines.[188]

Outsourcing cyber regulations to private corporations

---

[183] Rusbridger and MacAskill, 'Edward Snowden Interview'.
[184] Commisioner for Human Rights, 'The rule of law on the Internet and the wider digital world', (version: 8 December 2014) https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2734552&SecMode=1&DocId=2262340&Usage=2 (16 January 2016), 16.
[185] American Civil Rights Union, 'Testimony of Jameel Jaffer and Laura W. Murphy'.
[186] Greenwald and MacAskill, 'NSA'.
[187] J. Risen and E. Lichtblau, 'How the U.S. uses Technology to Mine More Data More Quickly' *The New York Times,* 8 June 2013.
[188]Human Rights Watch, 'With Liberty to Monitor All', *Human Rights Watch* (version: 28 July 2014) https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and (09-03-2016).

The leaked documents of Edward Snowden highlighted the close relationship between the U.S. government and some of the biggest U.S. tech companies. Some of the documents reveal that the NSA has far-reaching ties within Silicon Valley. Companies like Microsoft have actively collaborated with the NSA and offered the agency easy access to their data.[189] A top-secret 2013 budget request for Signal Intelligence (Sigint) of 255 million dollar shows the importance of this intelligence program that is focussed at influencing the IT industries and their encryption standards.[190] The document states that Sigint: "actively engages US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs" and that the program "insert[s] vulnerabilities into commercial encryption systems."[191] These vulnerabilities are then used by the NSA to crack encryption keys, which enables the NSA to tap into online communications.

Apart from law-based requests, The NSA also uses more indirect ways to ensure compliance of the ICT industry. One of the documents states that the NSA's commercial solution center, which assesses security software before presenting it to potential buyers in government agencies, uses its position to leverage software companies to build in back doors in their equipment.[192] The operation also made use of human intelligence through undercover agents. A leaked document of the GCHQ, a British intelligence agency that closely cooperated with the NSA on Sigint, states that one of its teams is "responsible for identifying, recruiting and running covert agents in the global telecommunications industry."[193]

Cooperation of Silicon Valley based organisations with the NSA results in a mutual beneficial relationship. According to two journalists of *The New York Times* the NSA has become one of Silicon Valley's largest customers of data analytics.[194] This is in line with the findings of professor Vincent Mosco, who has writes that "the Pentagon and U.S. intelligence agencies are an increasingly essential training ground for tech start-ups."[195] Internet scientist, Evgeny Morozov, sums up the relationship between the NSA and Silicon Valley as follows: "[A] decentralized system, run by the private sector and enabled by a social contract between Silicon Valley and Washington: while Silicon Valley runs, updates and monetizes the digital infrastructure, the NSA can tap IT on demand. Everyone specializes and everyone wins."[196]

---

189 G. Greenwald, 'Microsoft handed the NSA access to encrypted messages', *The Guardian,* 12 July 2013.
190 G. Greenwald, 'Revealed: how US and UK spy agencies defeat internet privacy and security', *The Guardian,* 06-09-2013.
191 Greenwald, 'Revealed: how US and UK spy agencies defeat internet privacy and security'.
192 Ibidem.
193 Ibidem.
194 J. Risen and N. Wingfield, 'Web's Reach Binds N.S.A. and Silicon Valley Leaders', *The New York Times,* 19 June 2013.
195 V. Mosco, *To the Cloud: Big Data in a Turbulent World* (New York 2014), (page no. unknown).
196 E. Morozov, 'The Price of Hypocrisy', *Frankfurter Algemeine Feuilleton,* 24 July 2013.

Censorship

Although the U.S. advocates freedom on the Internet, it would be wrong to assume that there are no instances of censorship at all. In 2009 Google started publishing a transparency report on requests to censor content in its search engine. From 2009 to 2014 the amount of U.S. government requests to delete online content has grown from 123 to 406 requests every six months. During the same period the amount of requests that were granted diminished from 80 to only 58.[197] Google reports the following example: "a court order requesting removal of dozens of pages written by a blogger about a local state scandal involving state politicians." Google didn't grant the request.[198]

Another example of U.S. censorship is when the U.S. authorities tried to get the website Wikileaks.org offline after the website started leaking sensitive and classified U.S. information. One week after the publication of the embassy cables all major U.S. financial firms unlawfully blocked all financial transactions to Wikileaks.[199] This blockade would continue for almost three years, completely ignoring the juridical principle of presumed innocence, and led to the loss of around 85 percent of Wikileaks income in the first few months after the financial blockade.[200,] At the same time there was a huge Distributed Denial of Service (DDoS) attack on the Wikileaks website leading its domain name provider to drop Wikileaks and its webhosting service to deny service to the website.[201]

According to Yochai Benkler, professor at Harvard Law School, these events where the direct result of senator Liebmans request towards private U.S. companies to cut Wikileaks off and are to be considered much more powerful than a legal approach. He writes:

> If we were to consider what judicial process would be required for the government to exert this kind of force directly . . . the barriers in law would have been practically insurmountable. However, the implicit alliance—a public- private partnership between the firms that operate the infrastructure and the government that encourages them to help in its war on terror, embodied by this particularly irritating organization—was able to achieve extra-legally much more than law would have allowed the state to do by itself. [202]

---

[197] Google, 'google-government-removal-requests', (Version: 18 January 2016) https://www.google.com/transparencyreport/removals/government/data/?hl=nl (18 January 2016).
[198] Google 'Explore Requests', (Version: 18 January 2016) http://www.google.com/transparencyreport/removals/government/notes/?hl=en-GB#authority=US&period=Y2014H1 (18 January 2016)
[199] Wikileaks, 'Mastercard Breaks Ranks in Wikileaks blockade' (Version: 03 July 2013) https://wikileaks.org/MasterCard-breaks-ranks-in.html (20 December 2015).
[200] S. Springer and H. Chi, 'Rethoric , Prejudice and Violance in the Face of Wikileaks' *Geopolitics* 17 (2012) 3, 681-711, 682 and R. Zajácz, "WikiLeaks and the problem of anonymity: A network control perspective." *Media, Culture & Society* 35 (2013), 489-505, 498.
[201] BBC News, 'Wikileaks Website Back Online After DDoS Cyber-attack', (Version: 14 August 2012) http://www.bbc.com/news/technology-19255026 (3 Februari 2016).
[202] Y. Benkler, 'A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate', *Harv. CR-CLL Rev.* 46 (2011) 342.

In the end these measures did not lead to the intended result of getting the Wikileaks website offline and could not stop the dissemination of the classified documents on the web. The U.S. authorities even tried to refrain people from accessing the public documents. Many federal agencies prohibited their personnel to read or access Wikileaks. Even universities send round memorandums to their students that reading the Wikileaks documents could influence their chance on employment. [203]

Furthermore although the U.S. is not actively censoring its citizens its all-encompassing surveillance apparatus does result in a general sense of being watched. *Freedom House* reports that one of the key developments in 2013-2014 has been self-censorship by journalists and writers as a result of online surveillance causing a lack of anonymity.[204] A research by *PEN*, an international literary and human rights organisation, indicates that 85 per cent of the writers participating in their study were concerned about government surveillance.[205] Respondents indicated that they were self-censoring on topics like: "Middle East North Africa region, mass incarceration, drug policies, pornography, the Occupy movement, […] and criticism of the U.S. government."[206] While the U.S. is not restricting Internet access or use directly, its mass-surveillance practices provide a certain extent of control to the U.S. authorities in the U.S. cyber domain.

Summary

While the U.S. is advocating a free and open Internet, the 9/11 attacks established a discourse of fear that led to the large-scale monitoring of the domestic Internet. The U.S. government has used existing legislation and implemented new legislation to enable its agencies to monitor information streams. A lack of oversight has resulted in a large-scale surveillance program that consolidated state power by intruding the privacy of U.S. citizens. This was partly possible, because the U.S. government had acquired a large influence in the ICT sector which it used to leverage tech companies to hand over data and build in backdoors to its software. Through these measures the U.S. was able to regain control over the complex information streams in its domestic cyber domain.

Because the U.S. is a liberal democracy it does not feel as threatened by free flows of information as China. As people have freedom of speech and believes, the U.S. generally doesn't censor the Internet. This research shows however, that exceptions can be made when the government's legitimacy is under serious threat. The past 15 years the government has regained some extent of control over its domestic Internet, but at the same time the Snowden revelations about its large-scale surveillance schemes have damaged its legitimacy.

---

[203] Benkler, 'A Free Irresponsible Press', 342-343.
[204] 'Freedom on the net 2014: United States', *Freedom House, 2.*
[205] PEN America 'Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor' (version: 12 November 2013) https://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf (15 January 2016).
[206] PEN America 'Chilling Effects'.

4.2 The influence of the Internet on U.S.' interdependence sovereignty

During a meeting with the National Security Telecommunications Advisory Committee (NSTAC) in March 2002 the president of the U.S. expressed concern over the ability to protect the edges of the Internet.[207] As the U.S. cyber domain exists of many interdependent networks that are for 90 per cent owned by private operators, the 'edge' of the U.S. cyber domain turned out to be very hard to identify.[208] A committee was appointed to define the edge of the Internet and concluded the following in a 2003 report:

> Defending—not defining—the national edge of the Internet is most important. Yet, defence of the Internet is a concept that is almost impossible, given that it implies that the Internet is defensible everywhere it touches—across every border around the world. The concept of a secure Internet will remain a global work in progress as it addresses a global dynamic problem.[209]

The conclusion of the report was that defining a single edge of the Internet would fall short of identifying all different fields where security systems should be in place in order to establish a secure U.S. cyber domain.[210] Over the past 15 years the U.S. have focussed on border control by protecting three different edges of the Internet: The global level, the private operator level and the federal networks. What measures did the U.S. government take to defend its interdependence sovereignty? And how successful has the U.S. been in regaining the control over the borders of its cyber domain?

Cross-border cooperation and International standards

When the first U.S. Cyberspace Strategy was published in 2003, one of the main priorities was to establish a transnational network in order to face cyber challenges. In the strategy the problem was recognized that the interconnectedness of the Internet meant that the computer in one continent could inflict great damage on a system in another continent.[211] The protection of U.S. borders therefore needed a global approach. The document stated that the U.S. relied on "international cooperation to share information related to cyber issues and, further, to prosecute cyber criminals. Without such cooperation, our collective ability to detect, deter, and minimize the effects of cyber-based attacks

---

[207] The President's National Security Telecommunications Advisory Committee, 'Internet security task force reports', (Version: 25 June 2003) https://www.dhs.gov/sites/default/files/publications/ISATF_Issue_2_final_0.pdf (24 January 2016).
[208] Betz & Stevens, *Cyberspace and the State,* 71.
[209] The President's National Security Telecommunications Advisory Committee, 'Internet security task force reports'.
[210] Ibidem.
[211] US-Cert, 'The National Strategy to Secure Cyberspace', (Version: Februari 2003) https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (26 January 2016).

would be greatly diminished."[212] It also emphasised the need to facilitate international partnerships in order to create a "global culture of security."[213]

In the 2015 U.S. cyber strategy of the Department of Defence (DoD) this is still one of the main recommendations. The Strategy focuses on building international alliances, informing international allies on cyber threats and assisting them to build capacity in the cyber domain. The document states:

> The pursuit of security in cyberspace requires a whole-of-government and international approach due to the number and variety of stakeholders in the domain, the flow of information across international borders, and the distribution of responsibilities, authorities, and capabilities across governments and the private sector.[214]

The DoD recognizes the complexity of securing the national cyber borders in an environment where the national cyber domain is made up of thousands of networks that are owned by both national and international governments and private actors. Because the DoD doesn't have enough cyber capacity to engage with all international actors, it mainly focuses on the most strategic regions, like the Middle East and key NATO allies.[215]

One of the government bureaus that plays an active role in building International alliances is the Bureau of International Narcotics and Law Enforcement Affairs (INL) who promotes the cooperation of international agencies to strengthen International law enforcement. It lobbies for U.S. standards in policies on cyber crime in multilateral forums. The INL works on international capacity building and helps to establish legal frameworks for countries that do not have sufficient legislation in place yet.[216] As the exact borders of the U.S. cyber domain are hard to identify, the U.S. government aims to create a safer global cyber environment, in which it can combat trans-border crime according to U.S.-standards.

Public Private Partnerships

In the first U.S. cyber security strategy of 2003 the U.S. government writes that private organisations play an essential role in securing the U.S. Internet. In the report George Bush states that the

---

[212]US-Cert, 'The National Strategy to Secure Cyberspace', 8.
[213]Ibidem, xii.
[214] The Department of Defense, 'The DoD Cyber Strategy', (Version: April 2015) http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (28 January 2016).
[215] 'The Department of Defense, 'The DoD Cyber Strategy'.
[216]U.S. Department of State, 'Cyber crime and intellectual property crime', http://www.state.gov/j/inl/focus/combatting/cybercrime/ (26 January 2016).

cornerstone of U.S. cyber strategy is the public-private partnership.[217] The nation's critical infrastructure is made up of both private and public organisations that provide critical services, like water supply, banking and emergency services and therefore private organisations have played a key role in establishing cyber security since 2003.[218] The report also admits that large portions of the Internet are owned by the private sector, which leaves the responsibility to protect these parts of the Internet in the hands of private operators.[219] It is therefore desirable that there will be a system in place that facilitates information sharing between Private and Public institutions. [220]

The key role that the private sector plays in cyber security is still very much apparent in 2011 cyber policy, which states that "Cybersecurity is a shared responsibility across the public and private sectors."[221] In the latest cyber security strategy, published in 2015, the private sector is even called the "first line in defence" in cyber security, as private operators control ninety per cent of the Internet.[222] These private networks are identified as one of the edges of the U.S. cyber domain and the DoD emphasizes the responsibility of the private organisations to protect their own networks by implementing basic security measures. According to the DoD most cyber threats will be stopped by these basic security measures, leaving the U.S. government to deal with the most dangerous attacks.[223]

The 2015 cyber strategy differs from previous cyber strategies in that there is much more emphasis on the role that the private sector could play in the exchange of technical knowledge and the building of capacity in the governments cyber defence program. The DoD explicitly states it wants to employ technical experts from the IT-industry to help shape the DoD's cyber defence. It also speaks about exchange programs of the DoD with the private sector to get more technical knowledge on board.[224]

Defending federal networks

Apart from defending the edge of the U.S. cyber domain by improving the global cyber security and by cooperation with the private sector, the U.S. government has a program to defend the networks at the gates of the U.S. federal agency networks. The responsibility to protect the online federal infrastructure lies with the Department of Homeland Security (DHS). DHS has created a program called Einstein that monitors government networks. The program consists of three sub-programs:

---

[217] US-Cert, 'The National Strategy to Secure Cyberspace', 1.
[218] Ibidem, 1.
[219] Ibidem, ix.
[220] Ibidem, 20.
[221] Executive Office of the President National Science and Technology Council, 'Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program', (Version: December 2011) https://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf (28 January 2016).
[222] The Department of Defense, 'The DoD Cyber Strategy', 5.
[223] The Department of Defense, 'The DoD Cyber Strategy', 5.
[224] The Department of Defense, 'The DoD Cyber Strategy', 18.

Einstein 1 and 2 monitor data travelling from and to the federal networks, while Einstein 3 is the more sophisticated sub-program that can actively block incoming data at ISP-level.[225]

Einstein 1 was developed in 2003 by DHS and functioned as an early warning system for civilian government agencies that could install a sensor that was capable of detecting malicious code. The participation in the program was, however, voluntarily and in 2006 only a few of the agencies had joined the program.[226] With the Obama administration coming into power in 2008, the voluntary aspect of the Einstein program ended. The Obama government took on a more top-down approach to cyber security and obliged all federal agencies to take part in the Einstein 2 program. [227]

Einstein 2 was a more sophisticated version of the Einstein 1 program in which the monitoring of incoming and outgoing data was enriched with a deep-packet inspection, which allowed the sensor to not only monitor but also analyse the data that was passing through the main gateways of the federal agency networks.[228] This new type of data handling was only possible because the Obama administration had drastically reduced the amount of external network gateways. This allowed for more expensive and sophisticated technology at the main gateways that connected the federal agencies to the backbone of the Internet.[229]

In 2010 the third Einstein sub-program was launched, which next to deep packet inspection could also block harmful data-streams from entering the secured network of the federal agencies. The technology of Einstein three was developed by the NSA, which resulted in privacy concerns among the general public.[230] Especially when Einstein 3 was offered to major defence contractors and three Internet service providers were taking part in a pilot using Einstein 3. This led civil liberty advocates to protest that the use of Einstein 3 could result in major government led surveillance programs.[231] Currently the Einstein 3 program is still an important way for the U.S. federal agencies to assure network security.[232]

---

[225] M. Derosa, "The tension between Privacy and Cyber Security", *American Foreign Policy Council* 8 (2013) 4-7, 5.
[226] M. Mueller and A. Kuehn, 'Einstein on the Breach: Surveillance Technology, Cybersecurity and Organizational Change', *Paper Prepared for the 12th Workshop on the Economics of Information Security* (11-06-2013) http://www.econinfosec.org/archive/weis2013/papers/MuellerKuehnWEIS2013.pdf (28-01-2016), 9.
[227] Mueller and Kuehn , "Einstein on the Breach", 12.
[228] Ibidem, 9.
[229] Ibidem, 12.
[230] A. Kuehn, "Extending cybersecurity, securing private internet infrastructure: The US Einstein Program and its Implications for Internet Governance", *Springer Berlin Heidelberg* (2013), 5.
[231] E. Nakashima, "NSA allies with Internet carriers to thwart cyber attacks against defense firms", *The Washington Post*, 16 may 2011.
[232] Department of Homeland Security 'Einstein 3 accelerated', (version: 17 April 2015) http://www.dhs.gov/publication/einstein-3-accelerated (28 January 2016).

Summary

It is not easy to define where the border of the U.S. cyber domain is located. The U.S. Internet exists of many interdependent networks that are largely owned by private operators. To define the edge of the U.S. Internet, would be to fall short of addressing the complexity of the U.S. cyber domain. That is why from 2003 on the U.S. cyber strategy is made up of roughly three pillars: securitizing the global Internet, cooperating with private organisations to establish a secure Internet, and the defence of federal networks.

Since then, the U.S. government has worked to set international (legal) standards for cyberspace and helped strategic areas with capacity building in the cyber domain. It has established close cooperation with allies to work towards a more secure global Internet. It has also recognized the importance of cooperating with private operators, as they own large parts of critical infrastructure. Lately it has started to realize that the IT industry is a valuable resource for innovation and technical expertise that the U.S. government needs for securing its own networks. It has therefore started exchange programs and the sharing of best practices. Furthermore, the U.S. government has taken steps towards centralizing its networks in order to be able to secure its main gateways with more sophisticated techniques. This allowed the implementation of the Einstein 3 program, which is the first program that is able to block suspicious content from entering the secure networks and functions as a firewall for the U.S. federal networks.

In short, the U.S. has been working towards a significantly safer domestic cyber domain. Since 2003 a significant change is noticeable in the perception of cyber threats, which resulted in the realization that the U.S. networks were not designed with security in mind. Since that moment the U.S. government has worked towards more control over cross-border flows, especially by securing its own federal networks towards a more centralized and secure cyber environment.

4.3 The influence of the Internet on U.S.' Westphalian sovereignty

Westphalian sovereignty is based on the principal of non-intervention and the exclusion of external actors from domestic authority structures.[233] Foreign intervention of any kind negatively impacts the Westphalian sovereignty of a state. Betz and Stevens state: "the most obvious example of how cyberspace interacts with Westphalian sovereignty is in the exercise of compulsory cyber-power."[234] This means that any type of computer network operation that impacts the (electronic) assets of another state violates that states Westphalian sovereignty.[235] Cyber espionage and cyber attacks are common examples of how the Internet can impact Westphalian Sovereignty of states, but Westphalian

[233] Krasner, *Sovereignty, Organized Hypocrisy,* 20.
[234] Betz, *Cyberspace and the State,* 60.
[235] Ibidem 60.

sovereignty can also be eroded by invitation. In the latter case the state voluntarily trades a little of its exclusive authority for other benefits, like becoming part of international conventions or organisations.

It is especially the violation of Westphalian sovereignty by coercion or imposition that raises concerns to the U.S. government. From 2013 to 2015 the cyber threat was appointed as the "number one strategic threat" to the U.S.. This places cyber threats above terrorist threats for the first time since 9/11.[236] While the Internet was originally designed to facilitate data exchange between scientists, the exponential growth of Internet usage outpaced the development of its security mechanisms, leaving the U.S. cyber domain prone to attacks from external actors.[237] How is the U.S. government defending its domestic sovereignty from external influences? And how successful is it in keeping foreign intervention at bay?

Safeguarding a Multi-stakeholder approach to the Internet

One of the ways that the Internet affects the U.S. Westphalian sovereignty is by the U.S. taking part in ICANN. By being part of an organisation that has the authority to make decisions over the Internet, the U.S. is trading a small part of its authority over its network infrastructure for the convenience of a global domain name system. It can be argued however, that the U.S. still has more authority within the ICANN then any other state participating in the organisation.[238] Because the global Internet finds it origins in a network that was originally created by the U.S. department of defence, the U.S. used to operate much of the key components to the domain naming system, which linked domain names to web address numbers.[239] While the U.S. officially transferred this responsibility to ICANN, a non-profit organisation, which employed a multi-stakeholder system in 1998, the U.S. has kept a special relationship with ICANN through multiple arrangements that allowed it to influence ICANN's decisions.[240]

Other major stakeholders like China and Russia have long tried to gain more control over the Internet through ICANN. Together with other authoritarian states they have lobbied for replacing the multi-stakeholder model with a multilateral model, which would give them more autonomy over the Internet and would likely enhance their censorship and surveillance practices.[241] The U.S. government who is a big proponent of the multi-stakeholder model has always opposed this reform. After the Snowden revelations about the NSA spying program, however, the disproportional influence of the

---

[236] The Department of Defense, 'The DoD Cyber Strategy', 9.
[237] Ibidem, 1.
[238] S. Pettyjohn, 'Net Gain: Washington Cedes Control of ICANN', *Rand Cooperation* (Version: 10 April 2014) http://www.rand.org/blog/2014/04/net-gain-washington-cedes-control-of-icann.html (28 January 2016).
[239] L. Kruger, "The future of Internet Governance: Should the United States Relinquish its Authority over ICANN?", *Congressional Research Service* (version 03-11-2015) https://www.fas.org/sgp/crs/misc/R44022.pdf (29-01-2016), 1.
[240] Kruger, "The future of Internet Governance", 3.
[241] Pettyjohn, 'Net Gain'.

U.S. within the global domain of the Internet has been scrutinized.[242] Presumably this is one of the reasons behind the 2014 announcement that the U.S. wants to transition its stewardship role over ICANN to the global stakeholder community. While opponents within congress believe the transition of power is undermining U.S. control of the Internet, supporters of the transition believe it's a strategic decision that will restrain authoritarian regimes of claiming more power over ICANN.[243] China and Russia have been lobbying to transit important Internet governing functions to a multilateral institution like the U.N., where all countries would have an equal vote on how to shape global Internet policies.[244] The U.S. decision to transfer its responsibilities to the global stakeholder community secures the multi-stakeholder model of global Internet governance and is therefore in U.S. interest.

Countering cyber threats and cyber espionage

Apart from violation of Westphalian sovereignty by invitation, the U.S. has recently started to actively secure its Westphalian sovereignty from violation by coercion or infiltration. As the U.S. is growing increasingly dependent on the Internet by connecting all sorts of physical networks to the Internet, cyber attacks can be of great consequence for the functioning of its critical infrastructure.[245] While the 2003 U.S. cyber strategy already highlighted that the cyber domain is recognized as an important domain for U.S. security, it was not until 2009 that president Obama declared U.S. digital infrastructure a national security priority. In a speech on May 29th 2009 he stated: "From now on, our digital infrastructure -- the networks and computers we depend on every day -- will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority."[246] One of the first measures he took in order to reshape cyber security measures, was a 60-day Cyberspace policy Review of all federal government's cyberspace plans, programs and activities.[247]

---

242 Pettyjohn, 'Net Gain'.
243 Kruger, "The future of Internet Governance", 17.
244 K. Maher, "No, the U.S. Isn't Giving UP Control of the Internet", *Politico Magazine* (19 March 2014) http://www.politico.com/magazine/story/2014/03/control-of-the-internet-104830?o=1 (18 January 2016).
245 D. M. Hollis, "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command", *The United States Army* (Version: 29 June 2010) http://www.army.mil/article/41585/USCYBERCOM__The_Need_for_a_Combatant_Command_versus_a_Subunified_Command/ (29 January 2016).
246 B. Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure", *The White House* (Version: 29 May 2009) https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (29 January 2016).
247 J. R. Reagan, "Securing Cyberspace: National Security Strategy and Implications." (Version: 31 may 2014) https://www.researchgate.net/profile/Dr_Jr_Reagan/publication/262727881_Securing_Cyberspace_National_Security_Strategy_and_Implications/links/0deec538a1f271f8d2000000.pdf (29 January 2016).

In the same year U.S. defence secretary, Robert Gates, ordered the establishment of a sub-unified command that would unify all DoD's dispersed cyber defence initiatives under one command: USCYBERCOM.[248] The U.S. Cyber command had three main missions: Defending DoD networks, systems and information, defending the homeland against cyber attacks of significant consequence, and providing cyber support to military and contingency plans."[249] USCYBERCOM would function in addition to the DHS, which already had the responsibility for safeguarding all federal civilian networks.[250]

USCYBERCOM became the cyber arm of the DoD, but also closely cooperated with other federal agencies, like the NSA, in order to share technical expertise.[251] In 2011, the Pentagon released a new Strategy for Operating in Cyberspace, which was the third of its kind under the Obama administration, but was the first that was issued by the Department of Defense.[252] The strategy emphasised that the cyber domain should be operationalized as the 'fifth' warfighting domain - next to land, sea, air and space – and should be organized, trained and equipped so the DoD can take full advantage of its potential.[253]

According to a news article on the DoD website, USCYBERSOM is still getting up to speed: "by 2018 the sub-command will be fully operational, with 6,200 cyber forces that will allow the department to defend its networks, defend the nation and support combatant commanders."[254] In the DoD's latest cyber strategy document, published in 2015, it recognizes that there is still a lot of progress that needs to be made in order to secure the U.S. against cyber threats.[255] One of the major improvements that are scheduled is to design a complete new network structure for the DoD in which security aspects will be incorporated in the architecture.[256]

Another aspect that has been receiving great attention by USCYBERCOM is the development of offensive cyber capabilities. The cyber strategy of 2015 states: "In appropriate circumstances, and on order from the National Command Authority, we must be able to conduct offensive cyber

---

[248] M. Glenny, 'Who controls the internet?', *Financial Times* (Version: 08 October 2010) http://www.ft.com/intl/cms/s/2/3e52897c-d0ee-11df-a426-00144feabdc0.html (28 January 2016).
[249] The Department of Defense, 'The DoD Cyber Strategy'.
[250] Ibidem.
[251] Ibidem.
[252] Reagan, "Securing Cyberspace: 13.
[253] 'Department of Defense Cyberspace Policy Report', *Department of Defense,* https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (29-01-2016), 1.
[254] C. Pellerin, "Rogers: Data Manipulation, Non-State Actor Intrusions are Coming Cyber Threats", *The Department of Defense* (19 November 2015) http://www.defense.gov/News-Article-View/Article/630495/rogers-data-manipulation-non-state-actor-intrusions-are-coming-cyber threats (29 January 2016).
[255] The Department of Defense, 'The DoD Cyber Strategy', 1.
[256] C. Pellerin, "Cybercom Chief Details Strategic Priorities for 2016", *The Department of Defense* (Version: 21 January 2016) http://www.defense.gov/News-Article-View/Article/643954/cybercom-chief-details-strategic-priorities-for-2016 (29 January 2016).

operations."[257] There is a belief amongst the U.S. government that, as in many other domains, offense is the best defense.[258] Pentagon's cyber expenses on offensive capabilities are 2.5 times the amount of its defensive expenses.[259] USCYBERCOM commander, General Keith Alexander, stated in 2013 that the U.S. cyber offensive capabilities are "the best in the world."[260]

Summary

The origin of the Internet lies within the U.S. military networks and this has given the U.S. a disproportional role in the global Internet governance. As a result of the Snowden revelations and lobbying efforts of authoritarian regimes the role of the U.S. as steward of ICANN came under pressure. Rather than giving more control over Internet governance to other states, the U.S. is pressing for a bigger role for the multi-stakeholder community. Technically speaking, the U.S. government's authority of decision-making is not affected by this transfer, leaving its Westphalian sovereignty intact. The U.S. simply used its meta-political authority to transfer a piece of its authority to private organisations and NGO's, depoliticizing the subject.

The biggest concern for the U.S. is the violation of its Westphalian sovereignty by cyber threats and espionage. Most U.S. cyber strategy documents state that there is still much room for improvement in the cyber defence of the U.S.. Since president Obama came into power, there has been much more effort on reforming the federal cyber defence. One of the biggest reforms was the creation of USCYBERCOM that unified all dispersed cyber defence initiatives of the DoD. The responsibility of USCYBERCOM is to defend the nation against cyber attacks and to secure DoD networks against intrusion. In order to be able to defend the DoD networks a new single network infrastructure had to be build from the ground up, which integrated cyber security measures.

As the best cyber defence is considered to be cyber offence, USCYBERCOM is building capacity to implement offensive cyber attacks. In 2013 the USCYBERCOM commander, Alexander, was confident enough to state that U.S. cyber offensive capabilities where the best in the world. While the U.S. Westphalian sovereignty has been challenged by several cyber attacks in the past years, the U.S. has put great effort in improving its cyber defence, militarizing cyber space in order to maintain its Westphalian sovereignty in cyber space. USCYBERCOM is still being expanded and with cyber threats being categorized as the number one threat to the U.S. The coming years will reveal to what extent the U.S. is capable of fending of these types of attacks.

---

[257] The Department of Defense, 'The DoD Cyber Strategy', 5.
[258] P.W. Singer and A. Friedman, "Cult of the Cyber Offensive" *Foreign Policy* (Version: 15 January 2014) http://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/ (29 January 2016).
[259] Singer and Friedman, "Cult of the Cyber Offensive".
[260] Hearing before the subcommittee on Intelligence, emerging threats and capabilities "Operations: Modernization and Policy Issues to support the Future Force" (Version: 13 March 2015) https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg80187/pdf/CHRG-113hhrg80187.pdf (29 January 2016), 87.

5. Conclusion

When commercial Internet usage gained momentum in the early 1990s, it was unclear what its impact would be on state sovereignty. Because cyberspace lacks borders and the very nature of the Internet dictates openness and facilitates information exchange, many scientists believed that the Internet would help the spread of liberal values across the world, eroding traditional borders and authority structures. Throughout the past two decennia however, both authoritarian states and liberal democracies have demonstrated that they are capable of erecting borders and control mechanisms in order to protect their state sovereignty against the rise of the Internet. The past five years have shown the tendency of both authoritarian and liberal powers to treat the cyber domain as an operational domain, like land, space and air, which needs to be secured against foreign threats.

In this paper I have analysed various policies and regulations regarding the Internet that China and the U.S. have implemented to secure their sovereignty in three of the four dimensions of sovereignty that are identified by Krasner: domestic sovereignty, interdependence sovereignty, and Westphalian sovereignty. The fourth dimension of sovereignty – International legal sovereignty – was never substantially threatened by the Internet and has therefore been left out of this research.

The different dimensions of Krasner's framework on sovereignty proved to be very helpful in structuring the various measures that China and the U.S. have taken to secure their sovereignty in the era of the Internet. The framework has helped to disentangle the different elements of sovereignty and to study them separately. This doesn't mean that it is undisputable which regulations and measures fall within each different dimension of sovereignty. One of the shortcomings of the framework is that the boundaries between the different dimensions are not always clear-cut, at times making it hard to decide which government policies and regulations belong to which dimension of sovereignty. Nevertheless, the framework provided a useful tool to study the complex concept of sovereignty and all its aspects in a structured and comprehensive way.

During the analysis I have found that both countries have identified threats to all three dimensions of sovereignty and actively opposed these threats by the implementation of cyber regulation, cyber policy and the militarization of cyber space. China recognized these threats as soon as it was connected to the Internet in 1994. For the U.S., the 9/11 attacks led to increased securitisation of the Internet. In order to protect domestic sovereignty from the influences of the Internet, both countries implemented a wide range of legislative measures that allowed the government to regain power over its domestic Internet. In addition, both countries executed large-scale surveillance operations to provide national security and to regain control over what was happening on the domestic Internet. Furthermore, both China and the U.S. closely cooperated with private organisations, which enabled the government to monitor Internet traffic and to gain access to data stored on their servers.

The two different political backgrounds of China and the U.S. led to two different perceptions of what threatened their state sovereignty. While the biggest threat to the domestic sovereignty of the Chinese government is anti-government sentiment and ideology, the biggest concern to the U.S. was the prevention of terrorist attacks in the aftermath of 9/11. The authoritarian nature of China resulted in the lack of any privacy restrictions and the ability of the Chinese authorities to gain as much information on its citizens as they perceived necessary to secure their sovereignty. The liberal nature of the U.S. meant that the U.S. could only implement large-scale surveillance programs after the 9/11 attacks, when the perceived threat of terrorism was bigger than the perceived threat of privacy violations.

The Chinese authorities felt threatened in their interdependence sovereignty by any type of information flow that could lead to questioning the legitimacy of the Chinese authoritarian government. This led the Chinese authorities to filter all information flows entering and exiting the country for keywords and blocking information accordingly, which was only possible because the Chinese government had created a Chinese Internet infrastructure in which each entry-point was controlled by the government.

Although the U.S. feels the need to secure its federal networks from unwanted border flows, the same type of border control of its Internet domain was impossible. As the U.S. had created its Internet infrastructure with openness, and not security, in mind, the U.S. cyber borders are much harder to define. In order to secure its borders, the U.S. aimed its policies towards creating a safer global Internet domain, close cooperation with private organisations and operators and securing its own federal networks with the Einstein program.

Apart from domestic- and interdependence sovereignty, the Internet challenged the Westphalian sovereignty of both China and the U.S.. China faced two types of erosion of its Westphalian sovereignty. On the one hand its Westphalian sovereignty was eroded by invitation, as it had to share its authority over the Internet according to the multi-stakeholder model of ICANN. While conducting this research, however, China seemed to be successful in lobbying for a new approach to Internet governance that would lean more towards a multilateral model in which its sovereignty on this matter would be restored. On the other hand, the Chinese government identified threats to its Westphalian sovereignty by infiltration. It has built a cyber security force with offensive capabilities in order to face these threats, while making use of the technological expertise of the IT-industry. The biggest threat to its Westphalian sovereignty however, is not considered to be cyber attacks or cyber espionage but the threat that the Internet poses to its social stability. Till now, the Chinese government has gone to great lengths to shield off its Internet against these ideological threats and has been relatively successful in blocking ‘harmful’ ideological content from entering its cyber domain through the Great Firewall of China.

As the U.S. had a stewardship role over ICANN, it could exert more power over the global Internet governance than other countries participating in ICANN. Although the U.S. government was under pressure from the international community to take a step back, it has used its power to leverage for a solution that would give more power to the multi-stakeholder community, which would likely lead to a more favourable outcome for U.S. control than a more multilateral approach. The real threat to U.S. Westphalian sovereignty is not by invitation but by infiltration through impending cyber attacks. That is why the Obama administration has put much effort in unifying cyber defence and creating a more secure network structure. The private IT-industry is considered a valuable source for technical knowledge and indispensable for a successful cyber strategy. As offence is perceived to be the best cyber defence, considerable resources have gone into creating the best offensive cyber capabilities in the world.

Both countries faced ambiguities in their Internet policy and regulations that impeded their objectives to secure their state sovereignty on the Internet. While China wanted to limit interconnectivity of its citizens in order to avoid political influence by exposing its citizens to foreign values and ideology, it also wanted to stimulate economic growth and IT industries. In order to achieve this, the Chinese government had to accept that there had to be some extent of 'collateral freedom'. And while the U.S. was advocating an open and borderless Internet in order to facilitate the free flow of information, at the same time it had to secure itself against Internet threats from abroad, like the spread of terrorist-networks and cyber attacks.

Although the Internet has posed threats to all three dimensions of sovereignty, the latest developments show that China and the U.S. are using the characteristics of the Internet to re-establish their authority and control. China is piloting a social crediting system, which allows it to track its citizens' every move on the Internet. By rewarding citizens for responsible behaviour on the net with higher loans, they can exert unprecedented influence on their citizens' behaviour. The U.S. is looking into ways to make optimal use of the huge amounts of data that are generated on the web by doing big data analysis in order to identify (cyber) threats.

Apart from using the Internet to re-establish their power and control over the domestic environment, both countries have taken measures to operationalize the cyber domain as a domain of warfare. In order to secure their cyber territory from intrusion by cyber-spying and cyber-attacks they have build both defensive and offensive capacities in cyber space. This implies that both states are viewing their domestic cyber space as subject to their authority, ensuring their political primacy in this domain.

In sum, both countries faced serious threats to their sovereignty since they've connected to the commercial Internet. However, throughout the years they have identified the challenges that the Internet brought upon them and found ways to mitigate them. While there is a difference between what China and the U.S. consider 'political' - and therefore what they perceive as threats to their

sovereignty - there are some striking similarities in the way they have faced these threats and re-established their control over the Internet. Right now both countries explore ways in which they can utilize the Internet to strengthen their authority and control while operationalizing their cyber domains against foreign threats.

I would therefore like to conclude that an overall trend is visible in both countries in which the state authorities analyse and actively oppose the challenges of the Internet to the different dimensions of sovereignty by means of regulation, policy and militarization of the cyber domain. While both countries have created two very different discourses about Internet freedom, there are striking similarities in the way they address these challenges. Regardless of the different ideological values of China and the U.S., in the end securing state power and control over the Internet seems to be the main objective in both countries, which leads to the conclusion that realist theory is still very much applicable in contemporary political science.

Both China and the U.S however, are hegemonic powers and have a wealth of economic resources to invest in cyber regulation and security. In order to be able to come to a more general assumption about the relation of the Internet and state sovereignty, further research must be conducted on the measures that smaller countries with fewer resources have taken to oppose the challenges of the Internet to their sovereignty. Therefore, based on this research alone, it would be to soon to apply this conclusion to the international political arena as a whole.

References

Literature

- Arquilla, J., and D. Ronfeldt, *The Advent of the Netwar: The Future of Terror, Crime and Millitancy* (Santa Monica 2001).
- Benkler, Y., 'A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate', *Harv. CR-CLL Rev.* 46 (2011).
- Betz, D. & T. Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power* (London 2011).
- Bollier, D., 'The Rise of Netpolitik – How the Internet is Changing Politics and Diplomacy' (Version 2003), http://bollier.org/sites/default/files/aspen_reports/NETPOLITIK.PDF (03 January 2016).
- Castells, M., *The Rise of the Network Society* (Sussex 2010).
- Chang, A., 'Warring State: China's Cybersecurity Strategy', *Center for a new American Security* (Version: December 2014) http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang_report_010615.pdf (03-02-2016).
- Chiang, X., 'The Battle for the Chinese Internet', *Journal of Democracy* 22 (2011) 47-60,
- Choucri, N. and D. Goldsmith, 'Lost in cyberspace: Harnessing the Internet, international relations, and global security' *Bulletin of Atomic Scientists* 68 (2012) 2, 70-77.
- Crampton, J., 'Collect it All: National Security, Big Data and Governance', *GeoJournal* 80 (2015) 519-531.
- Cupples, J. and K. Glynn, 'Wikileaks, Illegal Legalities, and the Biopolitics of Collective Counter intelligence', *Geopolitics* 17 (2012) 3, 681-711.
- Demchak, C. and P. Dombrowski, 'Rise of a Cybered Westphalian Age', *Strategic Studies Quarterly* 5 (2011)1, 32-61.
- Derosa, M., 'The tension between Privacy and Cyber Security', *American Foreign Policy Council* 8 (2013) 4-7.
- Drezner, D.W., 'The Global Governance of the Internet: Bringing the State Back in', *Political Science Quarterly* 119 (2004) 3, 477-498.
- Eriksson, J. and G. Giacomello, 'The Information Revolution, Security, and International Relations: (IR)relevant Theory?', *International Political Science Review* 27 *(*2006) 3, 221-244.
- Ferdinand, P., 'The Internet, democracy and democratization', *Democratization* 7 (2000) 1, 1-17.
- Galloway, T., and Baogang, H., 'China and Technichal Global Internet Governance: Beijing's Approach to Multi-Stakeholder Governance within ICANN, WSIS and the IGF', *China: An International Journal* 12 (2014) 72-93.
- Hathaway, M., 'Connected Choices: How the Internet is Influencing Sovereign Decisions', *American Foreign Policy Interest* 36 (2014) 5, 300-313.
- Hinman, L.M., 'Esse est indicato in Google: Ethical and Political Issues in Search Engines', *International review of information ethics* 3 (2005) 20-25.
- Howard, P., S. Agarwal and M. Hussain, 'When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media' *The communication Review* 14 (2011) 3, 216-233.

- Jiang, M., 'Authoritarian Informationalism: China's approach to the Internet', *SAIS Review* 30 (2010) 71-89.
- Krasner, S. D., *Sovereignty, Organized Hypocrisy* (Princeton 1999).
- Lea, J., and Stenson, K., 'Security, Sovereignty and Non-State Governance "From Below"', *Canadian Journal of Law and Society* 22 (2007) 2, 9-27.
- Luck, E.C., 'Sovereignty, Choice and the Responsibility to protect', *Global responsibility to protect* 3 (2009) 1, 10-21.
- Lee, J., and Liu, C., 'Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China', *Minnesota Journal of Law, Science, and Technology* 14 (2012), 125-151.
- Mackinnon, R., 'Networked Authoritarianism in China and Beyond: Implications for global Internet freedom', *Liberation Technology in Authoritarian Regimes* (Version: 11 October 2010), http://iis-db.stanford.edu/evnts/6349/MacKinnon_Libtech.pdf (03-02-2016).
- McReynolds, J., 'China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy' *The Jamestown Foundation* (Version:16 April 2016) http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=43798&no_cache=1#.VrG5uXgmf3c (02 Februari 2016).
- Mosco, V., *To the Cloud: Big Data in a Turbulent World* (New York 2014),
- Mueller, M., and A. Kuehn, 'Einstein on the Breach: Surveillance Technology, Cybersecurity and Organizational Change', *Paper Prepared for the 12th Workshop on the Economics of Information Security* (11-06-2013) http://www.econinfosec.org/archive/weis2013/papers/MuellerKuehnWEIS2013.pdf (28-01-2016).
- Rodriguez, J.C., "Comparative Study of Internet Content Regulations in the United States and Singapore: The Invincibility of Cyberporn, A." *APLPJ* (2000) http://cyber.law.harvard.edu/ilaw/Speech/Rodrig.htm, (12-01-2016).
- Sassen, S., 'The Impact of the Internet on Sovereignty: Unfounded and Real Worries', in Christoph Engel and Kenneth H. Keller (eds.), *Understanding the Impact of Global Networks on Local Social, Politicaland Cultural Values* (Baden-Baden: Nomos, 2000), 195-201.
- Shackelford, S. J. , 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law', *Berkley Journal of International Law* 27 (2009) 1, 192-251.
- Springer, S., and Chi, H., 'Rethoric , Prejudice and Violance in the Face of Wikileaks' *Geopolitics* 17 (2012) 3, 681-711, 682 and R. Zajácz, "WikiLeaks and the problem of anonymity: A network control perspective." *Media, Culture & Society* 35 (2013), 489-505.
- Tai, Z., 'Networked Resistance: Digital Populism, Online activism, and mass dissent in China', *Popular Communication*, 13 (2015), 120-131.
- Thomson, J.E., 'State Sovereignty in International Relations: Bridging the Gap between Theory and Empirical Research', *Internal Studies Quarterly* 39 (1995) 2, 213-233.
- Tsui, L., 'The Panopticon as the Antithesis of a Space of Freedom: Control and Regulation of the Internet in China' *China Information* (2003) 17, 65-82.

- Walton, *China's golden shield: corporations and the development of surveillance technology in the People's Republic of China* (Quebec, 2001).
- Yang, G., 'Internet Activism & the Party-State in China', *Daedalus* 143 (2014), 110-123.
- Yuen, S., 'Becoming a Cyber Power: China's Cyber Security Upgrade and its Consequences', *China perspectives* 2 (2015) 53-58.

Primary sources

- American Civil Rights Union, 'Testimony of Jameel Jaffer and Laura W. Murphy before the Senate Judiciary Committee', (Version: 31 July 2013) http://nsarchive.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-111e.pdf (12-01-2016).
- American Enterprise Institute, "Cyber surveillance regulations: Is the United States asking China to accept a double standard?", (Version: April 2015) https://www.aei.org/wp-content/uploads/2015/04/Cyber-surveillance-regulations.pdf (12 January 2016).
- Arthur, C., 'NSA scandal: what data is being monitored and how does it work?' *The Guardian*, 7 June 2013.
- Bandurski, D., 'China's Cyber-Diplomacy', *China Media Project* (Version: 21 December 2015) http://cmp.hku.hk/2015/12/21/39527/ (06 January 2016).
- BBC News, 'China internet: Xi Jinping calls for cyber sovereignty', (Version: 16 December 2015) http://www.bbc.com/news/world-asia-china-35109453 (06-01-2016).
- BBC News 'China Issues new internet rules that include jail time', (version: 09 September 2013) http://www.bbc.com/news/world-asia-china-23990674 (26 December 2015).
- BBC News, 'Wikileaks Website Back Online After DDoS Cyber-attack', (Version: 14 August 2012) http://www.bbc.com/news/technology-19255026 (3 Februari 2016).
- China Law Translate "Counter-Terrorism Law (initial draft)" (Version: 08 November 2014) http://chinalawtranslate.com/ctldraft/?lang=en (26 December 2015).
- Chinese People's Liberation Army 'China's Military Strategy', (Version: 26 May 2015) http://english.chinamil.com.cn/news-channels/2015-05/26/content_6507716_6.htm (3 February 2016).
- Hearing before the subcommittee on Intelligence, emerging threats and capabilities "Operations: Modernization and Policy Issues to support the Future Force" (Version: 13 March 2015) https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg80187/pdf/CHRG-113hhrg80187.pdf (29 January 2016), 87.
- Human Rights Watch, 'How Censorship Works in China: A Brief Overview' (Version: August 2006) https://www.hrw.org/reports/2006/china0806/3.htm (03 January 2016).
- Human Rights Watch, 'With Liberty to Monitor All', *Human Rights Watch* (version: 28 July 2014) https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and (09-03-2016).
- Commisioner for Human Rights, 'The rule of law on the Internet and the wider digital world', (version: 8 December 2014)

https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2734552&SecMode=1&DocId=2262340&Usage=2 (16 January 2016), 16.

- Department of Defense Cyberspace Policy Report', *Department of Defense,* https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (29-01-2016), 1.
- Department of Defence, 'Department of defence strategy for operating in cyber space' (Version July 2011) http://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD%20Strategy%20for%20Operating%20in%20Cyberspace%20July%202011.pdf (31-11-2015).
- Department of Defence, 'Fact sheet: The department of defence (DoD) cyber strategy', (version: April 2015) http://www.defense.gov/Portals/1/features/2015/0415_cyber strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf (31-11-2015).
- Department of Homeland Security 'Einstein 3 accelerated', (version: 17 April 2015) http://www.dhs.gov/publication/einstein-3-accelerated (28 January 2016).
- Department of Homeland Security, 'Safeguarding and Securing Cyberspace', *Department of Homeland Security* (version: 19 January 2016) https://www.dhs.gov/safeguarding-and-securing-cyberspace (9 March 2016).
- Executive Office of the President National Science and Technology Council, 'Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program', (Version: December 2011)https://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf (28 January 2016).
- Fan, J., 'How China wants to Rate its Citizens' *The New Yorker* (03 November 2015) http://www.newyorker.com/news/daily-comment/how-china-wants-to-rate-its-citizens (24 December 2015).
- Florcruz, J., & L. Seu "From Snail Mail to 4G, China Celebrates 20 Years of Internet Connectivity" *CNN* (version: 24-04-214) http://edition.cnn.com/2014/04/23/world/asia/china-internet-20th anniversary/ (24-12-2015).
- Freedom House, 'Freedom on the Net 2012 - United States' (25 September 2012) http://www.refworld.org/docid/5062e8941d.html (12 January 2016).
- Freedom House, 'Freedom on the Net 2015: China', (version: 2015) https://freedomhouse.org/sites/default/files/resources/FOTN%202015_China.pdf (03 December 2016).
- Freedom House 'Freedom on the Net 2015' (Version: 2015) https://freedomhouse.org/report/freedom-net/freedom-net-2015 (10 January 2016).
- Freedom House, 'Freedom on the net 2014: United States' (Version: 2014) https://freedomhouse.org/sites/default/files/resources/United%20States.pdf (12 January 2016).
- Gladwell, M., 'Small Change: Why the Revolution Will Not Be Tweeted', *The New Yorker*, 4 October 2014.
- Glenny, M., 'Who controls the internet?', *Financial Times* (Version: 08 October 2010) http://www.ft.com/intl/cms/s/2/3e52897c-d0ee-11df-a426-00144feabdc0.html (28 January 2016).

- Google 'Explore Requests', (Version: 18 January 2016) http://www.google.com/transparencyreport/removals/government/notes/?hl=en-GB#authority=US&period=Y2014H1 (18 January 2016)
- Google, 'google-government-removal-requests', (Version: 18 January 2016) https://www.google.com/transparencyreport/removals/government/data/?hl=nl (18 January 2016).
- Greenwald, G., 'Microsoft handed the NSA access to encrypted messages', *The Guardian,* 12 July 2013.
- Greenwald, G., 'Revealed: how US and UK spy agencies defeat internet privacy and security', *The Guardian,* 06 September 2013.
- Greenwald, G. and E. MacAskill, 'NSA Prism program taps in to user data of Apple, Google and others' *The Guardian,* 7 June 2013.
- Hatton, C., 'China 'Social Credit'; Beijing sets up huge system' *BBC News* (Version: 26 October 2015) http://www.bbc.com/news/world-asia-china-34592186 (24 December 2015).
- Hearing before the subcommittee on Intelligence, emerging threats and capabilities "Operations: Modernization and Policy Issues to support the Future Force" (Version: 13 March 2015) https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg80187/pdf/CHRG-113hhrg80187.pdf (29 January 2016).
- Hollis, D.M., 'USCYBERCOM: The Need for a Combatant Command versus a Subunified Command', *The United States Army* (Version: 29 June 2010) http://www.army.mil/article/41585/USCYBERCOM__The_Need_for_a_Combatant_Command_versus_a_Subunified_Command/ (29 January 2016).
- Hudson, D. L., 'Hate Speech Online' *First Amendment Center* (version: 13 December 2002) http://www.firstamendmentcenter.org/hate-speech-online (12 January 2015).
- Human Rights Watch 'Freedom of expression and the Internet in China', (Version: 01-08-2001) https://www.hrw.org/report/2001/08/01/freedom-expression-and-internet-china (26-12 2015).
- Human Rights Watch, 'How Censorship Works in China: A Brief Overview' (Version: August 2006) https://www.hrw.org/reports/2006/china0806/3.htm (03 January 2016).
- Human Rights Watch, 'Submission by Human Rights Watch to the National People's Congress Standing Committee on the draft Cybersecurity Law' (Version: 4 August 2015) https://www.hrw.org/sites/default/files/supporting_resources/hrw_submission_draft_cybersecurity_law_082015.pdf (26 December 2015).
- Hunt, K., and Xu, C., 'China 'Employs 2 Million to Police the Internet'', *CNN* (version: 7 October 2013) http://edition.cnn.com/2013/10/07/world/asia/china-internet-monitors/ (2 January 2016).
- Information Office of the State Council of the People's Republic of China 'White paper (IV) – Basic Principles and Practices of Internet Administration', (version: 8 June 2010) http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207983.htm (26 December 2015).
- Keller, B., 'Dealing with Assange and the Wikileaks Secrets', *New York Times,* 26 February 2011.

- Kruger, L., "The future of Internet Governance: Should the United States Relinquish its Authority over ICANN?", *Congressional Research Service* (version 03-11-2015) https://www.fas.org/sgp/crs/misc/R44022.pdf (29-01-2016).
- Kuehn, A.,"Extending cybersecurity, securing private internet infrastructure: The US Einstein Program and its Implications for Internet Governance", *Springer Berlin Heidelberg* (2013), 5.
- Levin, D., 'At U.N., China Tries to Influence Fight Over Internet Control', *The New York Times,* 16 December 2015.
- Lum, T., "Human Rights in China and U.S. Policy: Issues for the 114th Congress", *Congressional Research Service* (Version: 24-03-2015) https://www.hsdl.org/?view&did=765959 (09-03-2016).
- MacAskill, E., and Branigan, T., 'Edward Snowden vows not to 'hide from justice' amid new hacking claims', *The Guardian*, 12 June 2013.
- Madhani, B., "CCIA Urges Senate To Improve Cybersecurity Information Sharing Act" *Computer & Communications Industry Association* (Version: 15 October 2015) http://www.ccianet.org/2015/10/ccia-urges-senate-to-improve-cybersecurity-information-sharing-act/ (13 January 2016).
- Maher, K., 'The New Westphalian Web', *Foreign Policy* (Version: 25 February 2013) http://foreignpolicy.com/2013/02/25/the-new-westphalian-web/ (06 January 2016).
- Moran, T.H., 'Cyber surveillance regulations: Is the United States asking China to accept a double standard?', *American Enterprise Institute* (20 April 2015) https://www.aei.org/publication/cyber-surveillance-regulations-is-the-united-states-asking-china-to-accept-a-double-standard/ (29 Decmeber 2015).
- Morozov, E., 'The Price of Hypocrisy', *Frankfurter Algemeine Fueilleton,* 24 July 2013.
- Nakashima, M., "NSA allies with Internet carriers to thwart cyber attacks against defense firms", *The Washington Post*, 16 may 2011.
- Obama, B., "Remarks by the President on Securing Our Nation's Cyber Infrastructure", *The White House* (Version: 29 May 2009) https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (29 January 2016).
- Open Net Initiative, 'China profile', (Version: 09 August 2012) https://opennet.net/research/profiles/china-including-hong-kong287 (05 January 2016).
- Nakashima, E., "NSA allies with Internet carriers to thwart cyber attacks against defense firms", *The Washington Post*, 16 may 2011.
- Pellerin, C., "Cybercom Chief Details Strategic Priorities for 2016", *The Department of Defense* (Version: 21 January 2016) http://www.defense.gov/News-Article-View/Article/643954/cybercom-chief-details-strategic-priorities-for-2016 (29 January 2016).
- Pellerin, C., "Rogers: Data Manipulation, Non-State Actor Intrusions are Coming Cyber Threats", *The Department of Defense* (19 November 2015) http://www.defense.gov/News-Article-View/Article/630495/rogers-data-manipulation-non-state-actor-intrusions-are-coming-cyber threats (29 January 2016).

- Pelroth, N., 'Chinese Hackers Circumvent Popular Web Privacy Tools', *The New York Times*, 12 June 2015.
- PEN America 'Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor' (version: 12 November 2013) https://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf (15 January 2016).
- Pettyjohn, S., 'Net Gain: Washington Cedes Control of ICANN', *Rand Cooperation* (Version: 10 April 2014) http://www.rand.org/blog/2014/04/net-gain-washington-cedes-control-of-icann.html (28 January 2016).
- Punyakumpol, P., "The great Firewall of China: Background" *Torfox: A Stanford Project* (Version: 01 June 2011) http://cs.stanford.edu/people/eroberts/cs181/projects/201011/FreedomOfInformationChina/author/pingp/index.html (27 December 2015).
- Reagan, J.R., "Securing Cyberspace: National Security Strategy and Implications." (Version: 31 may 2014) https://www.researchgate.net/profile/Dr_Jr_Reagan/publication/262727881_Securing_Cyberspace_National_Security_Strategy_and_Implications/links/0deec538a1f271f8d2000000.pdf (29 January 2016).
- Reporters Without Borders, 'Draconian Cyber Security Bill Could Lead to Internet Surveillance and Censorship', (version: 04 June 2012) http://en.rsf.org/etats-unis-draconian-cyber-security-bill-06-04-2012,42283.html (03 February 2016).
- Reuters 'Ant Financial Unveils China's First Credit-Scoring System Using Online Data' (Version: 27 January 2015) http://www.reuters.com/article/ant-financial-services-idUSnBw276582a+100+BSW20150128 (26 December 2015).
- Risen, J., and Lichtblau, E., 'How the U.S. uses Technology to Mine More Data More Quickly' *The New York Times,* 8 June 2013.
- Risen, J., and Wingfield, N., 'Web's Reach Binds N.S.A. and Silicon Valley Leaders', *The New York Times,* 19 June 2013.
- RNW Media, "Bloggers Open Borders for the Media" (Version: 14 January 2016) https://www.rnw.org/articles/bloggers-open-borders-for-the-media (22 January 2016).
- Ryan, Y., 'Anonymous and the Arab Uprisings', *Aljazeera,* 19 May 2011.
- Sanger, D.E., and Perlroth, N., 'NSA Breached Chinese Servers Seen as Security Threat', *The New York Times,* 22 March 2014.
- Reporters Without Borders, 'Draconian Cyber Security Bill Could Lead to Internet Surveillance and Censorship', (version: 04 June 2012) http://en.rsf.org/etats-unis-draconian-cyber-security-bill-06-04-2012,42283.html (03-02-2016).
- Rusbridger, A., and MacAskill, E., 'Edward Snowden Interview – the edited transcript', *The Guardian,* 18 July 2014.
- Sanger, D.E., and Perlroth, N., 'Senate Approves a Cybersecurity Bill Long in the Works and Largely Dated', *The New York Times*, 27 October 2015.

- Singer, P.W., and Friedman, A., "Cult of the Cyber Offensive" *Foreign Policy* (Version: 15 January 2014) http://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/ (29 January 2016).
- Seiffert, J. 'Weighing a Schengen zone for Europe's Internet data', *Deutsche Welle*, 20 February. Department of Defence, 'Department of defence strategy for operating in cyber space' (Version July 2011) http://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD%20Strategy%20for%20Operation-%20in%20Cyberspace%20July%202011.pdf (31-11-2015).
- Schnurer, E. B., 'E-stonia and the Future of the Cyber State', *Foreign affairs,* 28 January 2015.
- Sutter, J.D., "The faces of Egypt's 'Revolution 2.0'", *CNN,* 21 February 2011.
- Svensson, M., "Internet in China and its Challenges for Europe: Dealing with Censorship, Competition and Collaboration." *ECRAN* (version: August 2014) http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=4935884&fileOId=5044735 (02-02-2016).
- The Electronic Frontier Foundation, "Patterns of Misconduct: FBI Intelligence Violations from 2001 – 2008" (version: 23 January 2011) https://www.eff.org/wp/patterns-misconduct-fbi-intelligence-violations#8 (15 January 2016).
- Tiezzi, S., 'China vows no compromise on cyber soveregnty', *The Diplomat* (Version 16 December 2015) http://thediplomat.com/2015/12/china-vows-no-compromise-on-cyber-sovereignty/ (06 January 2016).
- The Economist, 'How does China censor the Internet?' (Version: 21 April 2013) http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-china-censors-internet (27 December 2015).
- The President's National Security Telecommunications Advisory Committee, 'Internet security task force reports', (Version: 25 June 2003). https://www.dhs.gov/sites/default/files/publications/ISATF_Issue_2_final_0.pdf (24 January 2016).
- The White House 'International Strategy for Cyberspace', (Version: may 2011). https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (13-01-2016).
- US-Cert, 'The National Strategy to Secure Cyberspace', (Version: Februari 2003) https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (26 January 2016).
- U.S. Department of State, 'Cyber crime and intellectual property crime', http://www.state.gov/j/inl/focus/combatting/cybercrime/ (26 January 2016).
- U.S. Department of State, 'Internet Freedom', http://www.state.gov/e/eb/cip/netfreedom/index.htm (09 January 2016).
- Wikileaks, 'Mastercard Breaks Ranks in Wikileaks blockade' (Version: 03 July 2013) https://wikileaks.org/MasterCard-breaks-ranks-in.html (20 December 2015).