Hertie School

Content control contestations:

How and why internet governance norms emerge and develop

Berlin, Fall 2021

Daniëlle Flonk

Dissertation submitted to the Hertie School
in partial fulfilment of the requirements for the degree of

Doctor of Philosophy (PhD)

in the

Berlin Graduate School for Global and Transregional Studies

Advisors

First advisor
Prof. Dr. Markus Jachtenfuchs
Hertie School

Second advisor
Prof. Dr. Jan Aart Scholte
Leiden University

Third advisor
Prof. Daniela Stockmann, PhD
Hertie School

Summary

In the early days of the internet, it was often assumed that the internet would develop into a free and open technology. However, governments have proven to be able to govern the internet, control its content, and develop international content control norms. This dissertation looks at content control from an international norms perspective and asks: *How and why do international content control norms emerge and develop?*

I adopt an analytical eclecticist approach that combines elements from comparative politics and international relations. There are three aspects to this eclectic theory of content control. First, states subscribe to content control norms, which can range from liberal to illiberal norms. States cooperate in the area of content control and promote content control norms. Second, states support content control norms to a different extent because of the democratic or authoritarian values they subscribe to and their internal decision-making procedures, which can lead to conflict. Third, regional and international organizations affect the norm promotion strategies of states.

I use both qualitative methods (case studies, content analysis) and quantitative methods (negative binomial hurdle model) to answer the research question. In order to answer the *how* part of the research question, I analyze two aspects of content control norm development. First, I assess the broader conflicts over norms and institutions in internet governance. I show that these conflicts are dependent on the identities of the actors involved. Second, I analyze the strategies that autocratic states use to push for specific content control norms. I show that institutional structures create opportunities and constraints to their norm promotion strategies. In order to answer the *why* part of the research question, I zoom in even further by comparing content control practices between democratic and authoritarian regimes. I show that democracies also control content, but mainly security-related content. Hence, content control practices are dependent on the regime type identity of actors and the type of content targeted.

This dissertation shows that existing global internet governance models are contested and countermodels are emerging. These developments point towards the beginning of the end of the open and liberal internet order as we know it.

Acknowledgments

My PhD journey has been a long one and would not be complete without acknowledging all those I've seen along the way. It starts with Bertjan Verbeek for planting the idea of doing a PhD in the first place and helping me with getting a position, with Alex Lehr for showing me the beauty of quantitative research (and models), and with Thomas Eimer for countless discussions about (the decreasing) anarchy in the digital space.

A special mention should go to Bram Geurkink for always supporting me academically and in my private life, even when times were challenging. Also, my parents for always supporting me in continuing to learn and study throughout my entire life, and working so hard to enable me to get there. I want to thank my aunt and uncle for their support and for always showing interest in my work. Finally, I want to thank my friends in the Netherlands: Agnes Akkerman & Bertjan Verbeek (especially for the beschuit and all those great Japanese postcards!), Yaël van Drunen, Thomas Eimer (I wish that I could have shown you this finished dissertation), Gijs Hablous, Jolieke Jongerden, Alex Lehr, Andy Sarlea, Arjuna Snoep, and Andrej Zaslove. For a long time, we have been separated during the pandemic, but with every call, talk, and message, it was as if you sent a small piece of home across the border.

I am grateful for so many things that this PhD has given me. For all the great friendships that I've made in academia: I especially want to mention Amelie Harbisch and Anke Obendiek (and I wish we could have closed our PhD chapters in more normal times), but also Christoph Abels, Robert Benson, Julien Bois, Burk, Maria Debre, Isabel Ebert, Martina Ferracane, Julia Fuβ, Lisa Garbe, Jörg Haas, Oleksandra Keudel, Cédric Koch, Ting Luo, Katya Rothermel, Frederik Traut, my colleagues from the Berlin Graduate School for Global and Transregional Studies and Hertie School PhD offices, and my colleagues from the Jacques Delors Centre and the Digital Governance Centre.

For the people who gave their feedback on this work one way or another: Tanja Börzel, Nicole Deitelhoff, Bram Geurkink, Sassan Gholiagha, Katharina Höne, Nora von Ingersleben-Seip, Markus Jachtenfuchs, Christian Kreuder-Sonnen, Martin Koch, Simon Munzert, Anke Obendiek, Julia Pohle, Pavel Satra, Jan Aart Scholte, Wolf Schünemann, Daniela Stockmann, Alexandros Tokhi, Daniel Trottier, Lora Anne Viola, Dwayne Winseck, and Michael Zürn, and a number of anonymous reviewers. Your comments were all helpful and this dissertation would have never looked the way it does now without my peers!

For the many places where I've presented my research: the American Political Science Association (APSA) Annual Meeting, the Annual Convention of the Belgian Association for

Political Science (VPW) and the Dutch Political Science Association (NKWP), the Authoritarian Politics and International Relations (APIR) Workshop at the Berlin Social Science Center (WZB), the Deutsche Vereinigung für Politikwissenschaft (DVPW) Conference, the European Consortium for Political Research (ECPR) General Conference, the European Multidisciplinary Conference on Global Internet Governance: Actors, Regulations, Transactions & Strategies (GIG-ARTS), the International Studies Association (ISA) Annual Convention, the Joint PhD Workshop of the Berlin Graduate School for Transnational Studies and the Hebrew University of Jerusalem, and the Overlapping Spheres of Authority and Interface Conflicts in the Global Order (OSAIC) research group.

For the Deutsche Forschungsgemeinschaft (DFG) that funded my PhD research and prolonged my funding when times got difficult (FOR 2409, JA 772/8-1).

Finally, for my supervisors: Markus Jachtenfuchs, Jan Aart Scholte, and Daniela Stockmann. Thank you all for taking the time and effort to read and comment on my work. Markus, thank you for all the support and for sitting down with me frequently. Even weekly in the final stages of my dissertation. I can't count the times that I've gone into a meeting feeling lost and I left your office back on track.

The journey has been a long one, but it has not ended. Whereas it is with pain that I close this chapter, it is with joy that I will start a new one at the European University Institute.

Berlin, 31 July 2021

Table of contents

List of tables

List of figures

List of abbreviations

APEC	Asia-Pacific Economic Cooperation
ARF	Association of Southeast Asian Nations Regional Forum
ASEAN	Association of Southeast Asian Nations
BRICS	Brazil, Russia, India, China, South Africa
CIS	Commonwealth of Independent States
CoE	Council of Europe
CSTO	Collective Security Treaty Organization
DDoS	Distrbuted Denial of Service
EC	European Commission
ECO	Economic Cooperation Organization
EU	European Union
G8	Group of Eight
G20	Group of 20
GDP	Gross Domestic Product
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communication technology
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IO	International organization
IS	Information security
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITR	International Telecommunication Regulations
NA	Not applicable
NGO	Non-governmental organization
OECD	Organisation for Economic Co-operation and Development
OEWG	Open-ended Working Group
OONI	Open Observatory of Network Interference
OSCE	Organization for Security and Co-operation in Europe
ПРОКСИ / PROKSI	Противодействие криминалу в информационной среде / Countering crime in the information sphere

RATS	Regional Anti-Terrorist Structure
RO	Regional organization
SCO	Shanghai Cooperation Organisation
START	National Consortium for the Study of Terrorism and Responses to Terrorism
UK	United Kingdom
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNGA	United Nations General Assembly
UNGGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
UNHRC	United Nations Human Rights Council
UNSC	United Nations Security Council
US	United States
V-Dem	Varieties of Democracy
WEF	World Economic Forum
WIC	World Internet Conference
WCIT-12	World Conference on International Telecommunications
WSIS	World Summit on the Information Society

CHAPTER 1

Introduction

Daniëlle Flonk

I. Research problem & research question

There is an emerging societal debate about the openness of the internet and content regulation. More and more of our public discourse, cultural production, and social interactions take place online (Gillespie, 2018, p. 6). The actors that are able to control this content can therefore have a great influence on society and human interaction. A well-known example is the Chinese 'Great Firewall', which is an extensive internet censorship regime (Roberts, 2018). However, content control also takes place in democracies. Some forms of content control might be seen as justified, such as the limitation of hate speech in Germany (Breindl & Kuellmer, 2013). Other forms of content control are more contested. For instance, Spain blocked websites on a large scale during the 2017 Catalan independence referendum (Ververis et al., 2021). All these policies affect public discourse and social interaction, albeit in different ways and to a different extent. Content control is a balancing act and often a slippery slope, potentially leading to a limitation of freedom of speech. A critical assessment of content control norms and practices is therefore paramount to protecting freedom of speech online, the openness of societal debates, and, by extension, liberal democracy.

In the early days of the internet, it was often assumed that the internet would develop into a free and open technology that would be difficult to regulate (Barlow, 1996). However, scholars show a return of the state in internet governance (Haggart et al., 2021). For instance, autocracies censor the internet to prevent social mobilization (King et al., 2013b). In democracies, there is also a public demand for restricting internet content (Hintz & Milan, 2018a), for instance in response to riots, protests, and terrorism (Meserve & Pemstein, 2018, pp. 246–248). Hence, against initial popular and academic belief, states are increasingly able to govern the internet (Drezner, 2004, p. 478) and control its content (Deibert & Crete-Nishihata, 2012, pp. 341–343).

Content control is no longer an exception, but a global norm in emergence (Breindl, 2013; Deibert et al., 2010). For instance, states define internet censorship broadly or want to protect freedom of speech online. This dissertation aims to study how and why these content control norms emerge and develop. I define content control as the process by which actors with a given identity use different techniques, policies, and justifications to influence or limit access to internet content for a given purpose. Norms are shared standards of appropriate behavior for actors with a given identity (Finnemore & Sikkink, 1998, p. 891). Content control norms can justify illiberal practices in both democracies and autocracies. Hence, emerging illiberal content control norms can limit freedom of speech online and threaten liberal democracy. However, the

literature fails to adequately explain these developments. For instance, existing research on content control mainly focuses on techniques of control (King et al., 2013b; Murdoch & Anderson, 2008) or domestic content control policies (Goldsmith & Wu, 2006; Kalathil & Boas, 2003; Rodan, 1998, 2004; Wacker, 2003). This dissertation takes content control out of a domestic vacuum and looks at it from an international norms perspective. Therefore, the research question of this dissertation is:

How and why do international content control norms emerge and develop?

Even though there is little research on international content control norms, this dissertation argues that they do matter. I depart from the assumption that shared international norms increase the legitimacy of content control practices. They normalize content control and provide guidance on appropriate behavior (Ambrosio, 2008; Yom, 2014). This holds for both democracies and autocracies since norms are an authoritative source of power (Beetham, 1991). In other words, states increasingly control content, which has a negative effect on freedom of speech online and leads to an increasingly bordered internet.

In order to answer the research question, I first set out its theoretical, methodological, and empirical relevance. Then, I conceptualize content control norms. After conceptualizing the phenomenon of interest, I present the sub-questions that allow me to answer the research question. The theoretical part then discusses my analytic eclectic theory of content control. After that, I briefly discuss the methodology and research design. Finally, I give an overview of the papers.

II. Relevance

Focusing on content control norms fills three knowledge gaps. First, theoretically, this dissertation relates to two main strands of literature: the general literature on internet governance, and a specific sub-set of the internet governance literature that is concerned with content control.

Earlier (mostly activist) works in internet governance were quite skeptical about the role of the state in internet governance (see, for instance, Barlow, 1996). They believed that internet communities should and could govern themselves without state intervention (Goldsmith & Wu, 2006, p. 140). However, already in the 2000s, scholars argued against exaggerating the global nature of the internet and in favor of looking at the role of state actors (Drezner, 2004; Goldsmith & Wu, 2006). Recent works show a clearer return of the state in internet governance (Haggart et al., 2021; Mueller, 2017). For instance, scholars explore how states try to limit

internet freedoms (Polyakova & Meserole, 2019; Powers & Jablonski, 2015) or shut down the internet (Freyburg & Garbe, 2018; Ruggiero, 2011). Some works even advocate the establishment of borders in cyberspace since "good fences are erected to make good neighbors" (Demchak & Dombrowski, 2011, p. 32). Mueller argues that what authors often refer to as internet fragmentation is actually an increasing attempt by states to align the internet with jurisdictional boundaries (Mueller, 2017, p. 3).

The literature refers to different concepts related to the role of the state in internet governance, such as alignment (Mueller, 2017), balkanization (Polatin-Reuben & Wright, 2014), fragmentation (Mueller, 2017), sovereignty (Schünemann & Kneuer, 2021; Stadnik, 2021), splinternet (Drake et al., 2016), and subjugation (Polatin-Reuben & Wright, 2014). All these works point towards the same direction: "widespread state attempts to exert greater control in internet governance." (Haggart et al., 2021, p. 243). This dissertation contributes to this agenda by showing that the role of states in controlling internet content is, indeed, increasing. States develop norms in international fora to increase their role in internet governance. I take this argument even further by showing the beginning of the end of the open and liberal internet order as we know it.

Even though internet governance is a policy field like any other, the literature on internet governance is still not systematically tied to the international relations literature. Most of the internet governance literature does not utilize core international relations and global governance concepts such as international cooperation, regime complexes, epistemic communities, or (the focus of this dissertation:) international norms. Some authors even argue that we need entirely new theories for studying internet governance (Choucri, 2012). There are some exceptions (e.g., Cowhey and Müller 2009; Drezner 2004; Murray 2011; Nye 2014; Farrell & Newman 2021). For instance, there is research on legitimacy and counterhegemony in ICANN (Cavalli & Scholte, 2021). Other authors assess complex governance and authority conflicts in data governance (Farrell & Newman, 2018; Obendiek, 2021) or have tried to map the internet governance regime complex (Mueller et al., 2007; Nye, 2014). Finally, some authors show attempts to develop global internet governance norms (Hurwitz, 2014). This dissertation ties in with this growing literature and refutes the argument that we would need new theories in internet governance. The internet can be seen as a policy field like any other (Palfrey, 2010).

When we zoom in on the issue area of content control, there have been a number of developments in the literature. First, earlier accounts of this research strand mainly focused on authoritarian states increasing their control of content, whereby many authors focus on autocratic practices of China (Han, 2015; Harwit & Clark, 2001; King et al., 2013b; Wacker,

2003) or the consequences of the Arab spring (Heydemann & Leenders, 2011; Yom, 2014; Yom & Gause III, 2012). Some accounts even argued that content control remains largely absent in democracies (Deibert et al., 2008). It is only recently that researchers started to more systematically assess the illiberal and authoritarian practices with regard to internet governance and content control in democracies (Michaelsen & Glasius, 2018). This dissertation relates to this emerging agenda by analyzing content control practices in democracies.

Much of the existing research is based on small-N case study or comparative case study research. Because it is challenging to get reliable data on internet censorship and content control on a global scale (or interpret the existing data), research is often limited to qualitative approaches. There are some accounts of comparing content control between states – most notably political regimes – on a larger scale. For instance, Bak et al. find that higher internet penetration rates lead to less repression, but that this effect is greater in democracies than in autocracies (2018). Boas shows that autocracies can censor the internet while still promoting internet development (2006). Meserve and Pemstein find that democracies also remove internet content in order to influence public opinion, reduce criticism of public officials, and bolster national security (2018, p. 246). From these studies, we know that the political regime of a state influences its content control policies and regulations. My dissertation adds to this agenda by comparing content control practices between regime types. The added value of such an approach is the discovery that regime types can be similar along some dimension of content control. These findings can lead to a more critical assessment of freedom of speech online in democracies.

Furthermore, much of the content control literature is about the practices of content control. For instance, authors look at internet shutdowns (Freyburg & Garbe, 2018), removal requests (Meserve & Pemstein, 2018), or repression (Bak et al., 2018). I argue that, until now, the literature has overlooked that an important part of effectively controlling content is the legitimation of those practices through international norms and institutions. Academic works often fail to acknowledge that content control has an important international norms component to it. Only recently have authors acknowledged the existence of a liberal information order (Farrell & Newman, 2021). The current information order is considered liberal because it supports a free flow of information across borders. The free flow of information was not only supported by a group of liberal states but also by private actors and civil society (Farrell & Newman, 2021, p. 3). However, this order is increasingly contested by both liberal and illiberal actors, for instance via the development of illiberal internet governance norms. Therefore, this dissertation looks at content control from an international norms perspective.

In sum, the internet governance literature increasingly acknowledges the return of the state in internet governance. The content control literature increasingly acknowledges illiberal content control practices and the emergence of content control norms. However, a systematic framework for conceptualizing and analyzing content control norms is missing. Therefore, I provide an integrated framework for explaining the emergence and development content control norms. Hereby, I integrate theoretical elements from comparative politics (on political regimes) and international relations (on international norms and institutions), which I complement with empirical insights from the internet governance literature.

Second, methodologically, this dissertation adopts a complementary methods approach by combining both qualitative and quantitative research methods. Whereas most constructivist research is dominantly qualitative, this research integrates quantitative methods and large-N data with content analysis. Therfore, this dissertation goes beyond existing content control studies that have mostly focused on small-N research and comparison. I start by applying case study research to broader conflicts on the openness of the internet. Then, I use content analysis that analyzes the strategies used by authoritarian norm entrepreneurs in different institutional contexts. Finally, I use a multilevel binomial hurdle model to assess the differences in content control practices between democracies and autocracies. By combining qualitative and quantitative research methods, this dissertation provides an extensive picture of content control. The qualitative methods help me to uncover the causal mechanisms behind norm promotion efforts, and conflicts over norms and institutions. The quantitative methods help me to compare all countries in the world and explain the differences between them. By employing this variety of methods, I can therefore more comprehensively answer both the *how* and the *why* parts of the research question than existing research has done so far.

Third, I provide an empirical contribution by shedding light on content control norms emergence and development that have remained under-researched so far. Whereas we know much about domestic content control practices in certain countries, we still know little about the international cooperation and norms dimension of these practices. Hence, it remains unclear how domestic content control practices translate to international norms, and conflicts between actors. Whereas we know much about content control practices in autocracies, there is little comparison between different regime types. Hence, it remains unclear to what extent there are differences in content control practices between democracies and autocracies, and how these differences can be explained. This dissertation looks at the content control differences and overlap between regimes and how this translates to international norms and institutions.

Throughout my dissertation, I provide empirical evidence of a return of the state in internet governance and – by extension – the contestation of the open internet order. Authoritarian states are increasingly pushing for illiberal content control norms (and sometimes succeed in doing so). Democracies are also shifting their positions from a more liberal internet governance model to one that increasingly limits content. An important driver of these shifting positions is the securitization of content, which enables regulation in democracies and creates common ground between democracies and autocracies.

Disentangling who controls what for which purpose, therefore, contributes to a more comprehensive understanding of content control policies and justifications. It allows citizens to be more critical of content control practices. It allows policy-makers in liberal democracies to dodge pitfalls such as the securitization of content. Hence, a critical assessment of content control can contribute to the protection of liberal democracy and freedom of speech online. One way of doing so is by framing content control debates not in terms of which content should be deleted or censored, but in terms of which content we find valuable and want to protect.

III. Conceptualizing content control norms

Before I explain the emergence and development of content control norms, I conceptualize this dependent variable. I set out my own conceptualization of content control. I define content control by assessing which tools actors use for which purpose. I show that these considerations for controlling content vary and therefore, content control should not be conceptualized as a binary, but as a continuum with several dimensions.

Deibert & Crete-Nishihata define information controls as "actions conducted in and through cyberspace that seek to deny, disrupt, manipulate, and shape information and communications for strategic and political ends." (Deibert & Crete-Nishihata, 2012, p. 343) Similarly, Weidmann & Rød define information control as "the government's ability to critically influence what is communicated on the Internet and how information is used. Establishing and maintaining Internet control is fundamentally a long-term strategy." (Weidmann & Rød, 2019, p. 31). The problem with these conceptualizations is that it is not very helpful for analyzing content control in the context of international relations. Although methods and techniques might differ between countries, this only becomes relevant to international relations theory when states start to communicate about and justify these methods via international norms. Therefore, I argue that a definition of content control should not only include the techniques that states use, but also the policies and how they justify these policies.

When we would conceptualize content control in such a way, the concept becomes more useful when analyzing content control as a global governance phenomenon.

I define content control as the process by which actors with a given identity use different techniques, policies, and justifications to influence or limit access to internet content for a given purpose.[1] I argue that there are four aspects that constitute content control: the layers in which content control takes place, the actors that control content, the aims of content control, and the different purposes of control.

First, there are several layers of content control: techniques, policies, and justifications. Techniques contain what is mainly addressed in the academic literature, such as filtering content, blocking websites, Distributed Denial of Service (DDoS) attacks, and surveillance (Deibert et al., 2008, 2010; Deibert & Crete-Nishihata, 2012). Policies are also slightly addressed by the existing literature, such as intermediary liability, defamation laws, registration legislation for Internet Service Providers (ISPs) and websites, and law enforcement with regard to cybercrime (Frosio, 2018; Tropina & Callanan, 2015). Hence, content control has technological and sociopolitical dimensions, and often if technological control is no longer possible, sociopolitical controls overtake them. For instance, when it is no longer possible to censor a blog post, a national government could decide to imprison the person responsible (Morozov, 2011, pp. 62–63). Or when hate speech is spread via social media, governments can hold companies liable for deleting such content. Besides these techniques and policies, content control also has a justification layer. They include justifications such as the protection of property rights, protecting national identity and uniformity, protecting children, and national security. Therefore, states develop international norms to justify national policies. I define norms as shared standards of appropriate behavior for actors with a given identity (Finnemore & Sikkink, 1998, p. 891). Since norms only prescribe behavior (and not a specific substance), content control norms can be liberal or illiberal, and democratic or authoritarian. An overview of these different layers can be seen in Figure 1, whereby we see a higher level of abstraction in higher layers.

[1] This definition is based on Deibert and Crete-Nishihata, who define information controls as "actions conducted in and through cyberspace that seek to deny, disrupt, manipulate, and shape information and communications for strategic and political ends" (2012, p. 343).

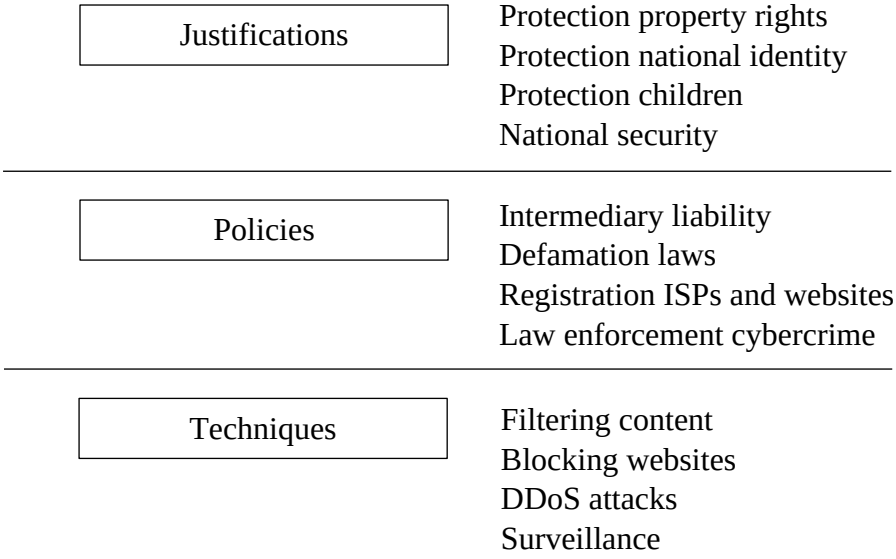


Figure 1. Layers of content control by states with examples.

Second, content control is pursued by actors with a given identity. These actors can be states, whether they are authoritarian or democratic. They can be private companies that attempt to limit or promote content. They can also be individual users themselves if they engage in self-censorship or DDoS attacks. There are a plethora of other actors who are capable of controlling content, such as non-governmental organizations (NGOs), forum moderators and administrators, or online communities.

Third, the aim of content control should be to influence or limit content. Influencing content is about adapting content itself by changing its message directly or indirectly. With regard to limiting content, actors can do two things: they either hide it or remove it (Gillespie, 2018, p. 175). Hiding content is about retaining content but limiting its delivery to certain users, with or without their knowledge (Gillespie, 2018, pp. 177–178). Removing content is an often-used approach since it is deemed effective and saves human resources for continuous moderation. However, it is also the most rigorous approach since it renders content invisible: "(r)emoval is a blunt instrument, an all-or-nothing determination, removing that content for everyone, not just for those who are offended." (Gillespie, 2018, p. 176)

Fourth, content control takes place for a certain purpose. Determining whether a measure is in the content control domain is not about its effect but its intention. Unintentional blockages (such as the cutting of a cable or a temporary loss of connectivity) might lead to the change or limitation of content. However, it becomes part of the content control domain once these measures are used intentionally: "(t)hey are there because somebody wants them to be there." (Mueller, 2017)

Hence, content control is applied in order to achieve strategic, social, economic, political, and legal goals. As I show in Chapter 4, differentiating between types of content is meaningful. In autocracies, the demand by governments for controlling political content is higher than in democracies. Autocracies also have fewer institutional constraints on controlling political content than democracies. However, the demand for controlling security content is often higher in democracies than in autocracies. In this policy area, democracies do not have more institutional constraints. Hence, the effect of regime type on content control is conditional on the type of content targeted.

Whereas political and security reasons are central to my dissertation, I do acknowledge that there are other reasons for control. Examples of such content include sexually explicit content, hate speech, self-harm, misogynistic content, racist content, homophobic content, trolling, harassment (Gillespie, 2018, pp. 36–37), gambling, and intellectual property rights (P. Pearce et al., 2017; Ververis et al., 2020, p. 2). These content examples can be categorized in several ways. Social sensitive content is often considered offensive, such as content "related to sexuality, gambling, and illegal drugs and alcohol" (OpenNet Initiative, n.d.). Hence, this type of content is dependent on social, cultural, and religious norms. I expect the demand for controlling this type of content would be higher in more authoritarian regimes. Content related to the information economy plays a role. For instance, states that are more invested in intellectual property production are also more likely to protect that property (Meserve & Pemstein, 2018, p. 259). Other economic interests also play a role in the push for more content control, such as the protection of communication services (e.g., countering Voice over IP) and gambling state monopolies (Breindl & Kuellmer, 2013, p. 372; Deibert et al., 2012). Hence, states that have a high interest in the information economy – such as the US – also have a higher demand for controlling this content. Hate speech and racial violence could be seen as another category. Especially in Germany and France, there is a discussion on the role of intermediaries in curbing hate speech and racial violence, since these countries have laws prohibiting Nazism, anti-Semitism, and white supremacy (Gillespie, 2018, pp. 57–58). Hence, it seems that the demand for hate speech control is high in most democracies. Finally, some content is universally contested, such as child abuse material or youth protection in the context of violence and sexually explicit content (Breindl & Kuellmer, 2013, p. 372; Deibert et al., 2012). In other words, there are several purposes of content control and some are seen as more legitimate than others, depending on the state or region in which it takes place.

Taking these four aspects of layers, actors, aims, and purposes together, content control is a continuum with different dimensions instead of a binary. Accordingly, international norms

can vary from taking into account human rights and an open internet on one extreme to a state-led internet and cybersovereignty on the other extreme. In academic debates, content regulation is often strongly linked with authoritarian control (Breindl et al., 2015, p. 29) pursued by authoritarian actors (Gomez, n.d.; Kalathil & Boas, 2003; Kerr, 2014, pp. 33–34; Rodan, 1998; Wacker, 2003). However, content control can also occur in democratic regimes (Deibert et al., 2010; Deibert & Rohozinski, 2010; Yangyue, 2014) under certain circumstances such as internal unrest (Meserve & Pemstein, 2018). Hence, content control is not a dichotomous concept (Bambauer, 2009b, p. 6) but a continuum on which the conception of appropriate control varies between actors with a given identity.

IV. Sub-questions

Describing and explaining the emergence and development of content control norms allows me to answer the research question. Therefore, I look more closely at the reasons for controlling internet content and at which country coalitions create, develop, and contest international content control norms. In order to answer the *how* part of the research question, I analyze two aspects of content control norm development. First, I assess the broader conflicts over the openness of norms and institutions in internet governance, in which content control norms are embedded. Second, I analyze the strategies that actors employ to push for specific international content control norms. In order to answer the *why* part of the research question, I zoom in further by comparing content control practices between democratic and authoritarian regimes, which helps me uncover their reasons for content control. This leads to the following sub-questions, on which I devote one chapter each:

How do states constitute spheres of authority in the area of internet governance and how does this translate to broader conflicts over norms and institutions? In Chapter 2, my research starts from a macro perspective on broader conflicts about the openness of the internet and the return of the state. I analyze how democratic and authoritarian regimes form spheres of authority that conflict over broader visions on internet governance norms and institutions. A sphere of authority is 'a governance space with at least one domestic or international authority, which is delimited by the involved actors' perception of a common good or goal at a given level of governance' (Kreuder-Sonnen & Zürn, 2020, p. 13). I show how adherents to the liberal and sovereigntist spheres of authority conflict over internet norms and institutions. These conflicts can reinforce but also contest the open internet order because it relates to the free flow of information and the role of state actors in internet governance. This chapter shows that content

control norms are part of larger conflicts on internet governance between proponents of spheres of authority.

How do illiberal norm entrepreneurs promote international content control norms via regional and international organizations? In Chapter 3, I zoom in on one specific illiberal country coalition. I assess the combination of socialization and persuasion strategies that authoritarian rising powers use for promoting content control norms. It shows that Russia and China change their content control norm promotion strategies based on the identity of their target groups and institutional surroundings.

How can the variation of internet content removal between regimes be explained, and which frames do states use to justify content control? In Chapter 4, I zoom in on content control even further by comparing content control practices between states. I explain the variation of content removal requests by governments to internet intermediaries and look at which reasons they have for controlling content. It shows that not only autocracies control content but that democracies also control content for specific security reasons.

V. Explaining the emergence of content control norms

In order to answer the main and sub-questions, I develop a theoretical framework that integrates comparative politics and international relations approaches. Comparative politics looks at the differences in content control practices and international relations assesses standards of appropriate behavior associated with those practices. These theories can increase our understanding of content control norm emergence and development. Hence, I adopt an analytical eclecticist approach that combines elements from comparative politics and international relations. The added value of adopting such an approach depends on how different mechanisms of existing research practices can be integrated as "elements of more complex explananda" (Sil & Katzenstein, 2010, p. 414). Hence, it makes an effort to articulate how different causal elements might coexist and make a more complex argument. In order to do so, one has to engage and utilize research by existing traditions. The purpose is to generate flexible frameworks organized around concrete problems. Hence, it is the problem that drives the construction of the framework (Sil & Katzenstein, 2010, pp. 414–415), not the theoretical paradigms embedded in research traditions.

Analytic eclecticism has three characteristics. First, it has a pragmatist ethos. Within pragmatism, there is a focus on the consequences of truth claims in concrete situations and social problems. Its principle is reconstruction, which is about updating scientific beliefs, habits, and practices in concrete situations (Sil & Katzenstein, 2010, p. 417). Second, problems are

formulated in such a way that they trace complexity rather than reduce it. Third, causal stories are focused on complex processes through which causal mechanisms interact. Hence, analytic eclecticism "offers complex causal stories that incorporate different types of mechanisms as defined and used in diverse research traditions." (Sil & Katzenstein, 2010, p. 419). Therefore, it seeks to trace the interactions between mechanisms across domains and levels of social reality (Sil, 2000, pp. 360–369; Sil & Katzenstein, 2010, pp. 416–419).

The starting point of this dissertation is therefore a societal problem at hand: increased content control and the emergence of content control norms. It signifies a clear return of the state in internet governance and the end of a truly open and liberal internet order. The internet governance literature acknowledges these shifts (Haggart et al., 2021; Mueller, 2017; Polatin-Reuben & Wright, 2014). The task of this dissertation is to paint a more complex picture of these causal stories and to trace the interactions between these mechanisms.

Therefore, the goal of this dissertation is not to provide a grand theory of content control. Instead, it operates on a more modest and pragmatic level of mid-range theories, "designed to be portable within a bounded set of comparable contexts where certain cause-effect links recur." (Sil & Katzenstein, 2010, p. 415) Analytic eclecticism serves two important purposes. First, it problematizes complex social phenomena instead of narrowly circumscribed puzzles. Second, it guides theories from multiple research traditions in order to establish linkages between mechanisms that are normally treated in isolation (Sil & Katzenstein, 2010, p. 426). Hence, it allows me to analyze the broader patterns behind a socially relevant development in internet governance, namely the return of the state and increased content control.

VI. An eclectic theory of content control

My main argument, therefore, starts at the point that all states control content. I argue that there are three aspects to an eclectic theory of content control. First, states subscribe to content control norms, which can range from liberal to illiberal norms. Content control is not only about practices but also about norms that justify those practices. Therefore, states cooperate in the area of content control and promote international content control norms. Second, states subscribe to content control norms to a different extent because of the democratic or authoritarian values they subscribe to and their internal decision-making procedures. Hence, the norms and decision-making procedures promoted in international institutions reflect domestic democratic and authoritarian values and decision-making procedures. However, this also leads to conflicts between states with different regime type identities. Third, regional and international organizations affect the behavior of states. Institutional surroundings (e.g., the

heterogeneity of member states) affect the norm promotion strategies of states. I will set out these arguments in more detail in the following section. I do so by using theoretical elements from the literature on constructivism, political regimes and liberalism, and neoliberal institutionalism.

First, content control is not only about practices but also about norms that justify those practices. Therefore, states cooperate in the area of content control and promote international content control norms. Even though the existing literature focuses much on domestic practices, there is a strong international relations component to the openness of the internet.

According to Finnemore and Sikkink, norms have a life cycle. When a norm is still at an early stage, norms are actively built and promoted by norm entrepreneurs (Acharya, 2004, p. 244; Finnemore & Sikkink, 1998, p. 896; Sunstein, 1996, p. 929), which are "agents having strong notions about appropriate or desirable behavior in their community." (Finnemore & Sikkink, 1998, p. 896) They are characterized by their proactiveness, call attention to issues, and frame issues in order to align them with public understandings or to understand issues in a new way. Norm entrepreneurs need an organizational platform from which they can act, such as regional and international organizations (Björkdahl, 2013, p. 325; Finnemore & Sikkink, 1998, p. 899). They need to find an organizational 'home' and negotiate broad support for a new norm (Björkdahl, 2002, pp. 50–51). Like traveling salespersons, norm entrepreneurs can resort to strategic venue change (or forum shopping) when discussions about a norm do not progress sufficiently in a certain institutional context (Björkdahl, 2002, pp. 50–51; Coleman, 2013, p. 164).

If norm entrepreneurs can push for new norms effectively, they will reach a tipping point after which they will spread. Norms will gain broader support and be internalized by target actors (Finnemore & Sikkink, 1998). However, since internet governance is an emerging field that is in flux and taking shape, content control norms are still in their emerging stage. This does not mean that this stage is without ambiguity, conflict, and different interpretations of how actors should behave according to the norm (Jose, 2017).

Second, conflicts over content control norms and institutional structures are dependent on the identities of actors involved in those conflicts. In this dissertation, I refer mainly to the identities of states based on their regime type. A regime is a "specific set of formal and/or informal rules for choosing leaders and policies." (Geddes et al., 2014, p. 314) Hence, a regime "determines who has access to political power, and how those, who are in power, deal with those who are not." (Fishman, 1990, p. 428) When determining regime types, scholars do not only assess whether countries have free and fair elections, but also whether they have liberal

values and freedoms that make these elections meaningful (Dahl, 1971, p. 8, 1998, p. 85; Lührmann et al., 2018, p. 3).

Liberal values affect to what extent freedom of speech online is protected, but also to what extent people are protected from illegal speech. Decision-making procedures affect how inclusive internet governance is and which societal groups can have an influence on policy outcomes. Hence, democracies and autocracies differ in their content control practices, since freedom of speech is more protected in liberal democracies and they are more inclusive. However, in certain policy areas (such as the fight against terrorism and crime), different regime types can have similar content control practices. This enables linkages between regimes and the formulation of common norms and practices.

I look at the role of political regimes in shaping international relations and the relationships between them. I argue that the dynamics behind conflicts over internet norms and institutions are very much a mirror image of the core elements of political regimes. Liberalism claims that "actors' domestic identities are crucial for their perceptions of one another in the international realm" (Risse-Kappen, 2016, p. 84), which has several assumptions. The fundamental agents in international politics are individuals acting in a social context. State interests have to be analyzed as a result of domestic structures and external factors such as the structure of the international system. Ideas are causally consequential in international relations. And international institutions form the social structure of international politics (presenting constraints and opportunities) (Risse-Kappen, 2016, pp. 82–83).

Hence, states' preferences over international outcomes are partly rooted in domestic political conditions (Tallberg et al., 2020, p. 6). Because democracy as a political system is based on liberal political ideas, democracies are more likely to favor liberal international outcomes than autocracies (Tallberg et al., 2016, 2020, p. 6). This dissertation argues that these liberal political ideas have two dimensions: ideas, values and norms, and decision-making procedures and institutional structures.

With regard to ideas, values, and norms, state perceptions are not derived from the international power structure but inferred from the values and norms governing domestic political processes that shape identities in the international system (Risse-Kappen, 2016, p. 84). Hence, the liberal values embedded in regime types can constitute collective identities among like-minded states (Risse-Kappen, 2016, p. 86). For instance, consolidated democracies have internalized democratic norms. Therefore, they bring these values and norms to the international institutions in which they operate (Dingwerth et al., 2015, p. 9; Grigorescu, 2010, p. 875). The

same argument could be made for autocracies, which are more likely to bring autocratic and illiberal norms to international institutions than democracies.

Hence, domestic identities and values determine state preferences. These preferences can be diverging or converging and, by extension, lead to conflict and cooperation between states (Moravcsik, 1997, p. 525). When national conceptions on values and norms are compatible between actors, they will likely cooperate. However, incompatible social identities of states create tension and conflict (Moravcsik, 1997, p. 525). One type of fundamental identity is the societal preferences on the nature and level of legitimate regulation (Moravcsik, 1997, p. 527). When underlying values converge, cooperation in regulatory issue areas is more likely. When there is more regulatory pluralism, conflict is more likely (Moravcsik, 1997, p. 528).

With regard to decision-making procedures, citizens in democracies expect that institutions should conform to democratic values. Therefore, they pressure their governments to push for democratic values, which adapt their discourse and practices accordingly (Dingwerth et al., 2015, p. 9). State preferences in international institutions are driven by norms of democratic governance (Grigorescu, 2010, p. 884). For instance, democratic norms can be applied to the functioning of international institutions. Discussions on democratic deficits and lack of accountability might lead to the increased participation of NGOs and broader access to information of the institution (Grigorescu, 2010, p. 875). In internet governance, the concept of multistakeholderism is based on deliberative and inclusive democracy. However, the same argument could be made for autocracies, which are more likely to push for decision-making to take place in institutions where states are the main actors.

Hence, domestic identities are based on perceptions of political legitimacy. Domestic liberal values and institutional structures of regimes affect the international norms and institutional structures that state actors pursue and subscribe to. Therefore, liberal theories are very much an international relations mirror image of theories on political regimes (see Figure 2).

International level	(Il)liberal international content control norms	International institutions: multistakeholderism vs. multilateralism; homogeneity vs. heterogeneity
Domestic level	(Il)liberal ideas, values, and norms embedded in regimes	Decision-making procedures: elections

Figure 2. The domestic-international mirror image affecting content control.

Third, from a neoliberal institutionalist perspective, I acknowledge the constraining and enabling role that international institutions have on state actors. Institutions are "persistent and connected sets of rules (formal and informal) that prescribe behavioral roles, constrain activity, and shape expectations." (Keohane, 2011, p. 159) A neoliberal institutionalist approach assumes that the institutionalization of world politics affects the behavior of states. Cooperation and conflict should be understood in the context of the institutions in which they take place. These institutional surroundings can have an effect in several ways, for instance by affecting the flow of information, monitoring, or managing expectations (Keohane, 2011, pp. 158–159). Hence, I show that states are not only influenced by their regime type, but also by the international institutions surrounding them. Institutions affect which norms states can promote, what their target groups are, and, as a consequence, which strategies they use.

In this dissertation, I argue that several structural elements play an important role in content control norm promotion strategies. One such structural element is the location or venue of norm promotion and development matters. I specifically focus on the differences between regional and international organizations. Norm entrepreneurs need a platform from which they can act (Finnemore & Sikkink, 1998). As I show in Chapter 3, regional organizations are often more homogeneous and therefore it is easier to develop norms in such a limited setting. International organizations are more heterogeneous and therefore norm promotion can become more challenging in such an environment. Norm entrepreneurs can even employ sequencing strategies whereby they first find support for a norm on a regional level, after which they spread the norm in an international organization.

Another structural element is the target audience of norm entrepreneurs, which matters for the strategies that they can employ. For instance, heterogeneous audiences are more difficult to convince of new norms than homogeneous audiences. This homogeneity can, for instance, be based on whether states belong to a liberal or sovereigntist sphere of authority (as I show in Chapter 2). It can also imply similarities between the regime types of states (as I show in

Chapter 3). When international organization membership is more democratically dense, audiences are more receptive to advocacy efforts in favor of liberal norms. In such a context, norm entrepreneurs face like-minded states that can support their norm promotion efforts. They will face fewer hurdles when trying to convince other members of a new norm (Tallberg et al., 2020, p. 6). Vice versa, when an international organization is more autocratically dense, audiences are more receptive to illiberal norms. Congruence also matters: if the identity of the norm entrepreneur aligns with the identity of the target audience, it makes norm promotion strategies easier. Hence, opportunities for and constraints on cooperation are partly defined by the level of convergence of preferences between states (Moravcsik, 1997).

This target audience aspect often interacts with the venue for norm promotion. For instance, regional organizations are more likely to be homogeneous than international organizations. Therefore, as I show in Chapter 3, norm entrepreneurs employ different norm promotion strategies in regional organizations than in international organizations.

Hence, this dissertation brings together the literature on constructivism, liberalism, and neoliberal institutionalism into an eclectic theory of content control. By combining the elements of these theories (i.e., international norms, regime type, institutional context), I come to a more comprehensive description and explanation of the emergence and development of content control norms. Furthermore, the integration of international relations theories allows for a more structural assessment of the internet governance field broadly and the sub-field of content control.

VII. Methodology

With regard to research design, this dissertation combines several approaches. In order to answer the *how* part of the research question, I employ two qualitative approaches. In Chapter 2, I employ case studies to track how conflicts over norms and institutions develop over time and what the outcomes of these conflicts are. This qualitative approach shows how content control norms are embedded in broader conflicts on the openness of the internet. In Chapter 3, I apply another qualitative approach by using content analysis and an illustrative case study. This research design allows me to expose how content control norms develop. It shows what discursive strategies illiberal actors employ to push for illiberal content control norms. In order to answer the *why* part of the research question, I turn to quantitative methods. In Chapter 4, I move to a quantitative research design to more rigorously compare the differences in content control practices between regimes. Furthermore, it allows for comparing the reasons for content

control on a large scale. In other words, I use a qualitative approach for describing and a quantitative approach for explaining the development of content control norms.

With regard to methodology, this dissertation employs different methods based on several data sources. My complementary approach applies qualitative and quantitative methods. Qualitatively, in Chapter 2, I (together with my co-authors) analyzed four cases that were selected because they are moments of intense debate where norm conflicts are activated. These cases are the World Summit on the Information Society (WSIS) and the Tunis Agenda from 2003 to 2005, the clash over seemingly technical details during the World Conference on International Telecommunications (WCIT-12) in 2012, the debates in the fifth session of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) in 2017, and the disputes over cybercrime and law enforcement online in the context of the Budapest Convention of the Council of Europe from 2017 onwards. The cases cover a wide scope of actors, issue areas, and time (more than fifteen years). We analyzed documents and trace conflict processes along several dimensions: the substantive content and context of the conflict, the conflicts over norms and institutions after the conflict was activated, and the outcomes of these conflicts.

In Chapter 3, I also apply a qualitative method, namely a large-scale content analysis. I collected 152 documents spanning over a ten-year period from two states, three regional organizations, and two international institutions. In these documents, I coded segments, uncovering the norm promotion strategies employed by Russia and China. In total, I coded 2,533 segments. Furthermore, I coded for each source the title, date, speech actor, organization, context (regional or global), and document type. All these documents were coded in MAXQDA (Plus 2020, release 20.4.0) in multiple iterations (see Appendix 1 for a list of codes). The complete MAXQDA database is available upon request. Finally, I use the proposals for a Code of Conduct for Information Security in 2011 and 2015 as an illustrative case study to show the mechanisms behind these norm promotion strategies.

Chapter 4 then moves into the realm of quantitative analysis. I use a unique dataset provided by Google on the amount and type of removal requests they receive from all countries in the world, allowing for cross-country comparison on a large scale and over time. In total, the data covers 240,151 items that were requested to be removed over seven years. I add independent and control variables to this dataset using data from Varieties of Democracies, the Global Terrorism Database, the Worldwide Governance Indicators, and the World Development Indicators. I estimate a negative binomial hurdle model to explain content

removal requests across regime types, using RStudio (version 1.0.153). See Appendix 4 for the R code written for data management, and Appendix 5 for the R code used for the analysis.

The combination of qualitative and quantitative methods allows for a comprehensive answer to the sub-questions and – by extension – to the overarching research question. This complementary methodological approach allows for addressing the research question step by step. With each chapter, I come to a higher level of granularity when describing and explaining content control norms.

VIII. Overview chapters

I address my main argument across three papers (see Table 1 for an overview). In Chapter 2, "Authority conflicts in internet governance: Liberals vs. sovereigntists?", I (together with my co-authors) assess these differences between political regimes from an international relations perspective by looking at distinct spheres of authority in internet governance. We assess how the democracies and autocracies constitute either a liberal sphere or a sovereigntist sphere that situate themselves in debates on global internet governance. Hence, we show how differences in domestic content control logic translate to international conflicts on internet governance norms and institutions. Different content control practices lead to content control norm promotion and conflicts, whereby we see clear attempts at competitive regime creation and regime shifting. This chapter aims to function as a point of departure by assessing the broader conflicts in internet governance, in which content control norms are embedded.

In Chapter 3, "Illiberal norms in emergence: Russia and China as content control promoters", I zoom in on two important actors of the sovereigntist sphere from Chapter 2 to show the causal mechanisms behind content control norm promotion. I argue that they combine socialization strategies in regional organizations and persuasion strategies in international organizations to promote information security norms (a Trojan horse for increased content control). In their promotion strategies, illiberal actors use security frames, which functions as a discursive bridge between the control of security and political content that is discussed in Chapter 4. Hence, autocracies try to exploit the security logic of content control present in democracies. Therefore, Chapter 2 and 3 both refer to the *how* part of my research question.

In Chapter 4, "Why governments control internet content: Comparing removal requests between regimes", I assess the *why* part of the research question. In this chapter, I zoom in even further to domestic content control practices. I show content control differences between countries, whereby I look at regime type as an explanation. It shows that democratic states are more likely to remove security content than closed autocracies. At the same time, they are quite

capable to protect political content that is critical of the government. Hence, I show that there is a security logic to domestic content control policies.

	Conflict over institutions	**Conflict over norms**	**Content control practices**
Main argument	International institutions reflect domestic decision-making procedures	International norms reflect domestic values and norms, constrained and enabled by institutions	Regimes have different reasons for controlling content
Theoretical framework	Liberal theory	Social constructivism, Liberal theory, Neoliberal institutionalism,	Political regimes, Liberal theory
Chapter	Chapter 2	Chapter 2, Chapter 3	Chapter 4

Table 1. Overview of chapters.

CHAPTER 2

Authority conflicts in internet governance: Liberals vs. sovereigntists?

Daniëlle Flonk, Markus Jachtenfuchs & Anke S. Obendiek

Abstract:

We analyze conflicts over norms and institutions in internet governance. In this emerging field, dispute settlement is less institutionalized and conflicts take place at a foundational level. Internet governance features two competing spheres of authority characterized by fundamentally diverging social purposes: A more consolidated liberal sphere emphasizes a limited role of the state, private and multistakeholder governance and freedom of speech. A sovereigntist challenger sphere emphasizes state control, intergovernmentalism and push against the preponderance of Western institutions and private actors. We trace the activation and evolution of conflict between these spheres with regard to norms and institutions in four instances: the World Summit on the Information Society (WSIS), the World Conference on International Telecommunications (WCIT-12), the fifth session of the United Nations Group of Governmental Experts (UNGGE) and the Budapest Convention of the Council of Europe. We observe intense norm collisions, and strategic attempts at competitive regime creation and regime shifting towards intergovernmental structures by the sovereigntist sphere. Despite these aggressive attempts at creating new institutions and norms, the existing internet governance order is still in place. Hence, authority conflicts in global internet governance do not necessarily lead to fragmentation.

I. Introduction

With its dramatic rise in importance, the analysis of internet governance increasingly moves from predominantly technical analyses to general conceptual lenses such as constitutionalization (Celeste, 2019; Fischer-Lescano, 2016; Pernice, 2018), the evolution of norms (Finnemore & Hollis, 2016) or the role of state interests (Drezner, 2007). We contribute to this mainstreaming by analyzing conflicts between spheres of authority in internet governance over the last 20 years.

We find that despite the relative novelty and the extreme dynamism of the field where one might expect to find rapidly evolving governance structures and complex conflict constellations, there is relative stability and only slow change of spheres of authority. A prevailing *liberal* sphere is strongly supported by Western states but increasingly challenged by an assertive *sovereigntist* sphere spearheaded by China, Russia and a number of authoritarian as well as developing countries. Contrary to what one might expect, the growing number of institutions and fora in internet governance and the explicit activation of norm collisions has not (yet) led to the fragmentation of internet governance. Rather, the liberal sphere is undergoing slow internal change.

Our argument proceeds as follows: In the next section, we present our understanding of internet governance, of authority conflicts and our methodology for selecting cases and analyzing these conflicts. The following four sections provide detailed studies of different cases for supporting our argument. We conclude by interpreting and generalizing the results.

II. Analytical concepts and methods

Defining internet governance has been subject to considerable debate by policy-makers (WSIS, 2005) and specialized scholars (DeNardis, 2014, pp. 19–20; Hofmann et al., 2017, p. 1418). As we aim to apply general concepts to the study of internet governance, we define (global) governance in line with a widespread use in international relations as ‘the exercise of authority across national borders as well as consented norms and rules beyond the nation state, both of them justified with reference to common goods or transnational problems’ (Zürn, 2018, pp. 4–5). This rather broad definition includes purely intergovernmental bodies as well as purely private or non-profit arrangements or mixed forms, and it refers to agreed norms and the exercise of authority (as opposed to power alone) but it is neutral with regard to the underlying social purposes.

Internet governance (like governance in other issue areas) takes place in distinct spheres of authority. A sphere of authority is more than just a group of like-minded states, which the

literature on internet governance frequently identifies (Deibert & Crete-Nishihata, 2012, p. 346; Maurer & Morgus, 2014, p. 3; Nye, 2014, p. 13), but 'a governance space with at least one domestic or international authority, which is delimited by the involved actors' perception of a common good or goal at a given level of governance' (Kreuder-Sonnen & Zürn, 2020, p. 13). Spheres of authority can comprise a diversity of actors such as states, intergovernmental organizations, private actors and multistakeholder fora, with some actors as focal points and some more at the periphery. In line with the definition of governance above, spheres of authority are not just functional or technocratic bodies but normative orders about common goods. For our empirical analysis, we distinguish between two ideal types, a *liberal* and a *sovereigntist* sphere. Our description emphasizes their characteristic and distinctive features. As ideal types, they are not meant to be an accurate representation of a complex reality but rather constitute an abstraction from this reality in order to use them as analytical concepts.

The proponents of the *liberal sphere* see the internet as an opportunity and as an emerging transnational space that should mostly be governed by private self-regulation based on voluntary participation and substantive expertise. Institutions should be flexible and stakeholder-based whereas the role of the state should be limited to providing security and enforcing hard rules when needed. Their social purpose is to encourage the development of the internet as much as possible by giving individuals, firms and civil society organizations as much freedom as possible. Intergovernmental organizations are perceived as too status-quo oriented for achieving this purpose. The underlying ideology is a combination of free market and pluralist civil society thinking.

The proponents of the *sovereigntist sphere* see the internet as a threat rather than as an opportunity. It should therefore be governed by intergovernmental institutions in order to respect domestic sovereignty and avoid external encroachments. Firms, civil society or experts should at best have an advisory role. The social purpose of this sphere of authority is to protect sovereignty and core domestic values and goals against domestic or international actors empowered by the internet. The underlying ideology is a world in which governments decide about domestic policies without external intervention and constraints and enter into international agreements on the basis of sovereign equality.

The added valued of constructing two competing views of internet governance stems from the fact that while there is often a myriad of social purposes, institutional architectures and social or legal norms, these highly specific elements often come in packages. As analytical concepts, our two ideal-typical spheres of authority are located at a rather high level of abstraction. There is room for variety within each sphere but no third way which is categorically

distinct from the liberal and the sovereigntist sphere. The libertarian views mainly popular in the 1990s as well as calls for tighter regulation and a more active state voiced in recent years are variants and possible trajectories of the liberal sphere.

Also, the diverging regulatory regimes of the US and the EU in the area of data privacy (Farrell & Newman, 2019) constitute struggles within it. The sovereigntist sphere encompasses the views of authoritarian states that wish to control the internet in order to maintain domestic rule as well as views of developing countries eager to have a greater say in a governance system they perceive as dominated largely by Western states and firms. When we speak of 'adherents' or 'proponents' of the liberal or the sovereigntist sphere, this is a shorthand for expressing the positions of states and other actors towards alternative ways of organizing internet governance. It does not say anything about their positions towards other issues and is not to be confounded with formal membership. Although the concept is neutral with regard to actors and could also include firms and civil society actors, we focus largely on states in this paper for reasons of space.

We use these two spheres of authority for understanding the evolution of conflicts about how internet governance should be organized. This shows the applicability of the concept of spheres of authority beyond established spheres (see Gholiagha et al., 2020) such as trade or drug control in rapidly evolving fields without a settled institutional structure like internet governance. We use our two ideal-typical spheres of authority for identifying stability, continuity and incremental change in a seemingly highly dynamic and unsettled policy area. We argue that underneath the surface of dynamism, the underlying social purposes, institutional preferences and norms remain relatively stable over time and are structured along a conflict line between two spheres of authority of which the liberal one is dominant and evolving over time while the sovereigntist one is a growing challenger.

For the analysis of these two spheres, we look at two dimensions where they clearly differ and where conflict is most pronounced. With respect to *institutions*, we analyze 'contested multilateralism' and assess state strategies in terms of whether they attempt 'regime shifting' (e.g., moving an issue from a multistakeholder forum to an existing intergovernmental institution) or 'competitive regime creation' (e.g., creating a new intergovernmental institution (Morse & Keohane, 2014)). The advocates of the liberal sphere prefer private or multistakeholder fora. They are not in principle opposed to formal institutions but support them in some cases, mainly for dealing with core state powers such as security provision and crime control. For these issues, they prefer Western organizations such as the Council of Europe. The sovereigntists want a different institutional setup that is not dominated by large and powerful

Western states and firms but gives primacy to sovereign states and equal representation and use regime shifting and competitive regime creation for achieving this goal. Their preferred institutional venue is the UN or its specialized organs such as the International Telecommunication Union (ITU).

With respect to *norms* (understood as shared standards of appropriate behavior for actors with a given identity; Finnemore & Sikkink (1998), p. 891), we analyze conflict over specific norms for governing the same substantive issues between the adherents of the two spheres, for instance whether they prefer to strengthen human rights and freedom of expression or rather stress norms of information security or criminal law. As is typical for internet governance, these norm collisions often involve general principles or social norms rather than hard law, which is the focus of other contributions in this Special Issue (e.g., Krisch et al., 2020; Moe & Geis, 2020). They often (but not exclusively) take place in political and deliberative fora rather than in institutions for formal law-making and adjudication. The proponents of the liberal sphere emphasize human rights, freedom of expression and a limitation of state control. Their sovereigntist contenders see the content of internet-based communication as a threat to domestic values and domestic stability that needs to be controlled rather than encouraged. Sovereigntists strive for the recognition and legitimization of state control over the internet. Table 2 provides an overview of the differences.

Conflict over	**liberal sphere**	**sovereigntist sphere**
institutions	- private or multistakeholder - institutional status quo - Western institutions - consensus-based inclusive deliberation	- intergovernmental - institutional change - UN or non-Western institutions - state veto power, one country/one vote
norms	- individual human rights - freedom of speech - free flow of information - universal values - unfragmented and global internet	- state rights - information security - territorial integrity, domestic stability - national sovereignty - national internet segments

Table 2. Spheres of authority in internet governance.

In order to trace developments over time and to analyze conflicts over norms and institutions in some detail, we provide four case studies on the conflict over the World Summit on the Information Society (WSIS) and the Tunis Agenda from 2003 to 2005, the clash over seemingly technical details during the World Conference on International Telecommunications (WCIT-12) in 2012, the debates in the fifth session of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) in 2017 and the disputes over cybercrime and law enforcement online in the context of the Budapest Convention of the Council of Europe from 2017 onwards. We selected these four instances of conflict because they are moments of high conflict and intense debate where norm conflicts are activated and competing institutional proposals are made. They show large shifts and breaks between the spheres of authority while covering a wide scope of actors, issue areas and time. They take place in different fora (a large UN conference, an international technical conference, a UN expert group and a European intergovernmental institution), cover highly different substantial topics (general principles of internet governance, technical norms, the role of international law and security issues) and stretch over more than 15 years. Showing that there is a constant pattern of conflict in highly divergent cases over an extended period strengthens the generalizability of the results.

In the following, we analyze the conflict presented above in a stylized form in more depth. We show that while some states changed sides during the evolution of the conflict and the substance of contestation shifted, the overall structure of two competing spheres of authority remained constant even in different issue areas. In the next four sections, we briefly describe the substantive content and context of each of the four instances, identify the most important conflicts over institutions and over norms after the conflict was activated and analyze the outcomes. A summary of our findings can be found in Table 3 (p. 37-38). Despite a series of intense challenges, there is still little fragmentation in internet governance and the existing order remains in place.

III. Emerging conflicts during the WSIS process and the Tunis Agenda

The first major conflict occurred at the first World Summit on the Information Society, which formally started at the International Telecommunication Union in Geneva in 2003 and continued in Tunis in 2005. With the burst of the dot-com bubble in 2000-2002, there was increasing recognition of a ‘regulatory void’ (Hofmann, 2005, p. 10) that needed to be filled. The development of regulative norms and principles as well as a definition of ‘internet governance’ became a key objective during the preparatory meetings and a Working Group on

Internet Governance was established. A group of sovereignty-oriented actors challenged the existing US-centric governance structures and the conference resulted in a compromise and established the UN Internet Governance Forum as a 'new forum for multi-stakeholder policy dialogue' (WSIS, 2005).

With regard to institutions, different perspectives existed concerning the status quo at the outset of the WSIS conference. The US-centric governance system included a multiplicity of rather informal, technical bodies, such as the Internet Engineering Task Force (IETF), private actors, and ICANN. The emerging countermovement, led by China, Brazil, South Africa and supported by the ITU, favored a more intergovernmental model (T. Wright, 2005), emphasizing the significance of political authority and its links to sovereignty and economic development (Kleinwächter, 2004).

While initially mostly favorable of the US model, the US unilateral oversight of ICANN, which existed at the time, increasingly developed into a source of conflict in the EU-US relations as well (Mueller, 2010, p. 74). In particular the simultaneous advertisement of private sector leadership was perceived as contradictory. Thus, a power battle emerged between the US and ICANN on the one side and both non-Western and European states on the other (Mueller, 2010, p. 67).

The European Commission (EC) proposed a 'new cooperation model' on 'a more solid democratic, transparent and multilateral basis, with stronger emphasis on the public policy interest of all governments' (EC, 2005) and thus implicitly questioned the status quo. It was severely criticized by the US as a concession to the sovereigntist push for an intergovernmental body (T. Wright, 2005). Multistakeholderism in its current form with relatively equal opportunities for the various stakeholders, particularly governments, was only emerging (Weinberg, 2011, p. 201). However, after significant diplomatic efforts, European and other democratic countries were willing to compromise due to concerns about the efforts by countries such as China, Saudi Arabia or Iran to increase cybersovereignty (Palfrey, 2010).

While there were significant divergences regarding the appropriate institutions for internet governance, there was less conflict over norms, probably because the low internet access rates in most but the highly industrialized countries kept issue salience low. Nevertheless, the narrative of the internet as a threat to domestic stability was already emerging. For instance, the Chinese representative's statement emphasizes the need to 'stress social responsibility and obligation' (Ju, 2005) in internet governance. In contrast, actors of the liberal sphere expressed concerns about threats to freedom of expression and emphasized principles of openness and participation as embodied by ICANN and the IETF as well as freedom of

expression and opinion as enshrined in the Universal Declaration of Human Rights (WSIS, 2005, p. 47).

The Tunis Agenda (WSIS, 2005) and the accompanying Tunis Commitment concluded the WSIS process with a compromise. On the one hand, the Tunis Agenda emphasizes that the '[p]olicy authority for Internet-related public policy issues is the sovereign right of States' (Art. 35a) and brings attention to governments' 'equal role and responsibility' (Art. 68). On the other hand, it legitimizes the existing structures (Art. 55) and, in a commitment to multistakeholderism, highlights the 'important roles' (Art. 35b, c) of private actors and civil society. The creation of the IGF as a forum for deliberation deescalated rather than resolved the conflict. Its weak institutional capacities, by some dismissed as a mere 'talkshop' (Zittrain, 2008), did not significantly restrict the authority of ICANN or other technical bodies. Therefore, the novelty of the IGF consisted in the significant inclusion of non-state actors in governance processes (Mathiason, 2008). Nevertheless, the creation of IGF already shows the emerging conflict between the liberal and the sovereigntist sphere.

With regard to norms, WSIS merely showed first signs of the conflicts that erupted later. The Tunis outcome documents often avoided specific phrasing on contentious issues to allow diverging interpretations by different countries and stakeholders (Mueller, 2010). However, in contrast to earlier discussions that emphasized less controversial 'bottom-up' processes, a commitment to a 'democratic' management of the internet featured prominently in the first paragraphs of the Tunis Agenda, which indicates that core norms of the liberal sphere prevailed.

After the conflict, the liberal sphere had further consolidated, despite the contradictions between the simultaneous emphasis on US government control and private sector responsibility. In contrast, the sovereigntist sphere was still in flux. The efforts of the democratic BRICS, in particular Brazil and South Africa, might have contributed to enhanced governmental responsibility in internet governance if the European states had backed their efforts towards increased transparency and public regulation (Ebert & Maurer, 2013). However, their insistence on the inclusion of private actors and concerns about the empowerment of authoritarian states made the Europeans join the US and push for multistakeholderism as an institutional compromise. This move successfully stopped the attempt to shift the regime to the UN.

IV. Fragmentation in a seemingly technical forum: WCIT-12

On the 2012 World Conference on International Telecommunications (WCIT-12), ITU member states wanted to amend the International Telecommunication Regulations (ITRs) treaty from

1988, which was widely regarded as outdated and unsuitable for dealing with growing threats of cybercrime, cyberwarfare, and cyberespionage. The ITRs established general principles about the provision and operation of international telecommunication services, and the underlying international transport means to provide these services (ITU, 1988). Although the ITRs were technical and most proposed revisions not controversial (about 90%, Hill (2013), 317), some proposals were highly conflictual. At the end of WCIT-12, 89 countries (under which many African countries, Arab states, China, Russia, Iran, and emerging economies like Argentina, Brazil, Indonesia, Mexico, South Korea, and Turkey) signed the revised ITRs whereas 55 countries (under which Australia, Canada, EU member states, India, Japan, New Zealand, and the US) did not sign the revised treaty (ITU, 2012b). This led to the creation of two institutional structures: one for the states which signed the revised 2012 ITRs and one for the states that stuck to the old 1988 ITRs (see Hill (2013) for a comprehensive overview).

There was strong disagreement between adherents of the liberal and the sovereigntist sphere over institutions (on the role of the ITU in internet governance) and norms (on the balance between human rights and security concerns). With regard to institutions, there was conflict over to what extent internet governance should be brought under UN auspices (Nocetti, 2015, p. 125). Whereas adherents of the liberal sphere wanted to keep the role of ITU limited, proponents of the sovereigntist sphere wanted to replace existing multistakeholder models by giving more authority to the ITU to regulate the internet. For instance, Russia submitted a proposal that member states should have equal rights to manage the internet with regard to naming and numbering (Russian Federation et al., 2012), aimed at creating an alternative to ICANN. Proponents of the liberal sphere were concerned that this kind of proposals would give more authority to the ITU and replace the multistakeholder model (US Majority Committee Staff, 2012). For the US, ‘to expand the ITR’s to include centralized control over the Internet through a top-down government approach would put political dealmakers, rather than innovators and experts, in charge of the future of the Internet’ (Verveer, 2012).

With regard to norms, states disagreed on human rights norms and the possible justification of content control. For instance, adherents of the sovereigntist sphere submitted a proposal that governments should know how internet traffic is routed and that operating agencies should determine which international routes should be used (Algeria et al., 2012, Art. 3) in order to improve cybersecurity. They also submitted a proposal about spam, defining it as information having no meaningful message transmitted in bulk over telecommunication networks (Russian Federation et al., 2012). Adherents of the liberal sphere were opposed to any proposal on cybersecurity and spam since this would have given national governments more

authority over the internet and justify internet censorship in the name of national security (US Majority Committee Staff, 2012). The US even wanted to prevent any mention of the internet in the revised ITRs because they feared limitations of freedom of speech online (Pfanner, 2012). As the US gained the support of the EU, a liberal and a sovereigntist bloc with strongly diverging preferences were in opposition.

The ITRs revision process escalated over the accompanying non-binding Resolution 3, which states that 'all governments should have an equal role and responsibility for international internet governance and for ensuring the stability, security and continuity of the existing Internet' (ITU, 2012a). Proponents of the liberal sphere were concerned that this would increase the role of the ITU and move internet governance more towards an intergovernmental model instead of a multistakeholder model (Hill, 2013, p. 325). The process by which this resolution was adopted is characteristic for the intensity of the conflict. Although the ITU Secretary-General had assured that no voting would take place, the conference chair, Mohamed Nasser al-Ghanim, asked for an informal poll, on which member states used their nameplates to show whether they agreed or not with the resolution. After a majority of member states was in favor of the resolution, the chair ruled that it was approved. Whether this process counted as an official and authoritative vote was debated until the end of the conference (Maurer & Morgus, 2014, p. 3). This incident activated the conflict and created concerns with adherents of the liberal sphere and greatly contributed to the later rejection of the revised ITRs by 55 countries.

In the end, 89 countries signed the revised ITRs, and 55 countries did not due to concerns over the ITU's role in global internet governance and increased state control over internet content even though there was a consensus that outdated technical regulations needed to be updated. Adherents to the sovereigntist sphere successfully created a competitive regime, which entered into force in 2015 for those ITU member states who signed the revised ITRs. For the non-signatories, the 1988 ITRs are still in force. WCIT-12 thus led to a fragmentation of internet governance in a specific sector.

V. Divisions over security at UNGGE 2016/2017

Since cybersecurity had become a global concern by 2015, the UN General Assembly (UNGA) tasked the fifth United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security (UNGGE) to write a report on how international law applies to the use of ICTs by states (UNGA, 2015b). The UNGGE was established after a Russian proposal in 2001 and consists of government representatives. Since 2004, five UNGGEs have convened on common norms, rules and

principles for responsible state behaviour in cyberspace. In 2013, the third UNGGE agreed *that* international law, and in particular the UN Charter, applied to the use of ICTs by states. The fourth UNGGE of 2015 articulated voluntary and non-binding norms of responsible state behavior (Tikk & Kerttunen, 2017, p. 11). However, during the fifth UNGGE in 2017, the working group could not reach a consensus on *how* norms of international law apply to cyber operations (UNGA, 2017b) and did not adopt its final report.

The conflict was activated when proponents of the liberal (the US and EU member states) and sovereigntist sphere (BRICS, Commonwealth of Independent States members and some developing countries) disagreed on a number of issues. Regarding institutions, adherents of the liberal sphere wanted to apply existing international law to cybersecurity without creating a new regime. However, adherents of the sovereigntist sphere preferred a new binding intergovernmental regime (Tikk & Kerttunen, 2017, p. 16) but proponents of the liberal sphere were unwilling to initiate such a negotiation process in the UN (Rodríguez, 2017).

Regarding norms, proponents of the liberal and sovereigntist sphere disagreed on what was concretely meant by the application of existing international law to issues such as the right to self-defence, countermeasures, and humanitarian law (Delerue, 2018, pp. 3–4). Adherents of the sovereigntist sphere feared that including the right to self-defence would legitimize retaliation with conventional weapons (Sukumar, 2017). Particularly problematic for them was the formulation in the draft final report that the malicious use of ICTs by states was the same as an armed attack as defined in Article 51 of the UN Charter (which justifies self-defence) (Rodríguez, 2017). Some states feared that the US would use such a reading of international law as a justification to launch retaliatory strikes against cyberespionage by countries like China (Segal, 2017, p. 7). They also feared that the reference to countermeasures could recognize the right to reciprocate a cyberattack (Sukumar, 2017). This would enable sanctions and punishment while bypassing existing mechanisms, such as the UN Security Council (Russian Federation, 2017). Since the US has superior conventional and cyber capabilities, the inclusion of the right to self-defence and countermeasures is problematic for sovereigntists (Sukumar, 2017). Moreover, they argued that a reference to Article 51 does not send a message of peaceful settlement of conflict prevention (Rodríguez, 2017) since it suggests a legitimation of cyberwarfare. Whether or not these are valid legal arguments is debatable but they show the high degree of conflict over the topic of cybersecurity.

These disagreements escalated once some proponents of the sovereigntist sphere started to retract their support for the applicability of international law made in previous UNGGEs. This backsliding was not acceptable for proponents of the liberal sphere. The US stated that

some participants believed that they are 'free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions' (Markoff, 2017). The diverging views between the two spheres' adherents proved to be insurmountable during the fifth UNGGE. The attempt of adherents of the liberal sphere to consolidate the existing information security regime failed when no final report was adopted. Likewise, the attempt of adherents of the sovereigntist sphere to shift the regime into their preferred direction or even creating a new regime failed when the UNGGE did not reach a consensus. Previously established reports were already fragile compromises and the chair of the fifth UNGGE, Karsten Geier, even argued that the establishment of a future UNGGE was unlikely since 'continuing to do the same thing and expecting a different outcome is a sign of madness' (Geier, 2018).

The divisions continued when conflicting resolutions by the US and Russia were both adopted by the UNGA First Committee in 2018. The US resolution (139 votes) calls for the establishment of a new UNGGE to further study norms and to discuss how international law applies to cyberspace (UNGA, 2018b). The Russian resolution (109 votes) establishes an open-ended working group (OEWG) to further develop the norms of the fourth UNGGE and to discuss models for regular institutional dialogue under the UN (UNGA, 2018c). This recent attempt by the sovereigntist sphere actors to create an alternative to the UNGGE is a development similar to the WCIT-12 case. It shows proactive attempts to create a competitive regime with the support of a considerable amount of countries and to move debates to new venues (e.g., the OEWG) when they are considered unfruitful in other fora (the UNGGE). Although the outcome of these developments are not clear yet, it at least indicates that the conflict between the proponents of the liberal and sovereigntist sphere over cybersecurity continues.

VI. Norm clash over cybercrime and law enforcement online

Cybercrime has become an increasingly significant global problem and is addressed by different global and regional institutions, such as the OECD, the G8, the African Union, or the Arab League. However, the Council of Europe's (CoE) (2001) Convention on Cybercrime (Budapest Convention), in force since 2004, is the only legally binding and arguably most important international instrument. The CoE is an intergovernmental organization focused on human rights, democracy and the rule of law in Europe. It has 47 member states, including all EU member states and Russia. The US and Canada have observer status. However, the Budapest Convention has explicitly been designed to have a global reach and at present has more than 60 parties to the convention, including the US, Canada, and Japan.

While not all CoE member states have ratified the convention, Russia is the only CoE member to refuse to even sign it, mainly due to concerns about cross-border law enforcement access during cybercrime investigations (CoE, 2001, Art. 32b). While the more intergovernmental character of the CoE should, in principle, find their support, sovereigntists under Russian leadership attempt to create a competing regime under the auspices of the UN that reflects a commitment to sovereignty and non-interference rather than strong human rights protections typical for the CoE. While Russia has been pushing for an international treaty in the area of cyber and information security since 1998, for instance at the UNGGE and other UN fora, these efforts are echoed by all BRICS states. The BRICS collectively stated after a meeting in late 2017 that they 'recognize the need for a universal regulatory binding instrument on combatting the criminal use of ICTs under the UN auspices' and 'acknowledge the efforts of the Russian Federation' (2017).

Russia activated the conflict by proposing a UN Draft Convention on Cooperation in Combating Information Crimes (Lavrov, 2017; Russian Federation, 2017) at the UNGA in 2017. While this proposal received only limited attention, a Russian-sponsored resolution, backed by Brazil, China and South Africa, was adopted with 88 votes in favor in November 2018 (UNGA, 2018a). Compared to the Draft Convention, the 2018 resolution is less ambitious but attempts to reemphasize the role of the UN, including the Secretary-General, in the area of cybercrime.

Most parties to the Budapest Convention reject these attempts as unnecessary or 'premature' (T-CY, 2017) in light of the existing framework and the significant time and effort necessary to negotiate a new agreement on the global level. The 2018 resolution was severely criticized by the US representative for its attempt at 'politicizing, polarizing and undermining' existing policies (US Department of State, 2018). In response to criticism of the exclusive negotiation framework of the CoE as a European institution, the CoE makes strategic efforts to appeal to particularly countries of the Global South through outreach and capacity building projects.

With regard to norms, the Russian-led efforts emphasize a commitment to cybersovereignty, territorial integrity and non-interference. For instance, Russian Foreign Affairs Minister Lavrov (2017) referred to a UNGA Resolution (UNGA, 2017a) emphasizing the right to non-interference and the rejection of extraterritorial use of national laws, which echoes criticisms of other sovereigntists. In contrast, proponents of the liberal sphere have voiced concerns about potential attempts to induce state control over the internet via a global treaty (UNGA, 2016). Whereas human rights online, such as freedom of speech or freedom of

opinion, are prominently mentioned in the Budapest Convention, they have a limited role in the Russian proposals or in the cybersecurity strategies of the SCO or China and are replaced by references to 'stability and security of society' or the need for sovereignty (China, 2017, Preamble). This conception of 'content as threat' for the internal stability of a country (Nocetti, 2015, p. 116; Palfrey, 2010) has been promoted increasingly since the Arab Spring by authoritarian countries. Liberal states consider these efforts as a 'Trojan horse' (Ebert & Maurer, 2013, p. 1055) to introduce content control and thus circumvent constitutionalist principles. This also decreased support from the democratic countries among the sovereigntists. This conflict is still ongoing.

VII. Conclusion

In this paper, we analyzed conflicts over norms and institutions in the field of internet governance. Beyond a multiplicity of seemingly unrelated issues, there is an overarching conflict between two fundamentally different views with different social purposes, institutional structures and specific norms (see Table 3 for an overview of our empirical findings). As internet governance is by and large not strongly legalized, this conflict rarely, and in contrast to other contributions to this Special Issue (see e.g., Krisch et al., 2020; Moe & Geis, 2020), involves collisions of legal norms from different established spheres of authority. Rather, it is in many instances not yet established which norms apply to which issue of internet governance. The UNGGE even debated whether international law was applicable at all. In this situation of normative uncertainty and rapid development, two distinct groups tried and are still trying to establish the applicability of specific norms to particular policy problems. In doing so, they draw on different sets of norms emanating from different institutions, the liberals typically from the area of human rights, the sovereigntists usually referring to non-interference and the collective rights of societies.

The polycentric nature of internet governance (Scholte, 2017), characterized inter alia by a low degree of legalization, the lack of a strong core institution or formalized dispute settlement, in contrast to other areas, such as world trade (see Gholiagha et al., 2020), and the rapid multiplication of formal and informal venues for dealing with internet governance, are factors that could have contributed to a quick fragmentation of internet governance. However, we find little fragmentation. Only one case can be interpreted as such. In the WCIT-12 case on the revision of the International Telecommunication Regulations (ITRs), a massive sovereigntist attempt at regime shifting was rejected by the adherents of the liberal sphere and led to the creation of a competitive parallel regime. The creation of the open-ended working

group (OEWG) by Russia in 2018 shows the resolve of the sovereigntists but it is too early to assess whether this is a permanent fragmentation.

		WSIS	WCIT-12	UNGGE	Budapest
Topic		definition, scope and actors of internet governance	revision of 1988 technical ITU Treaty for internet age	applicability of international law to use of ICTs by states	cybercrime convention
Forum		World Summit on the Information Society	World Conference on International Telecommunications	Fifth UNGGE (UN expert group)	Council of Europe, UN
Time of conflict		2003-2005	2012	2016/17	since 2017
Actors	**liberal**	US and ICANN, technical bodies; EU undecided and finally compromising	55 countries (incl. Australia, Canada, EU member states, India, Japan, New Zealand, US)	US, supported by EU member states and others	CoE members including US, but except Russia, Japan, South Africa
	sovereigntist	Brazil, South Africa, China, Iran and ITU with internal rifts due to democratic vs. authoritarian systems	89 countries (incl. African countries, Brazil, China, Indonesia, Iran and Russia)	BRICS states, CIS, developing countries	Russia, China, authoritarian countries (e.g., Iran), sometimes global South
Positions institution	**liberal**	private or multistakeholder body	maintaining multistakeholder model	no new regime, no multistakeholderism	globalize Council of Europe Budapest convention
	sovereigntist	UN, ITU	increasing role of ITU	creating a new intergovernmental regime	new UN treaty
Positions norms	**liberal**	freedom of expression	prevent increased authority of governments, prevent justification of content control, prevent mentioning internet in revised ITRs	apply right to self-defense, countermeasures and humanitarian law	human rights (esp. free speech), cooperation
	sovereigntist	first indications of content as threat	increased role of governments in governing	development of *lex specialis*, recognition of sovereignty in cyberspace	sovereign control, non-interference, for some: content control

		WSIS	WCIT-12	UNGGE	Budapest
			content, e.g., in traffic routing, defining spam		
Outcome	**institutions**	attempted sovereigntist regime shifting largely failed	successful sovereigntist competitive regime creation	attempted sovereigntists regime shifting failed, liberal consolidation of existing regime failed	ongoing attempts at sovereigntist competitive regime creation
	norms	commitment to democratic internet governance, but also emphasis on sovereignty	no agreement on government authority in internet governance	no consensus on *how* norms of international law apply to cyberoperations	ongoing clash between human rights and non-interference/content control norms

Table 3. Overview of conflicts and outcomes.

The underlying conflict between two spheres of authority is not limited to the four cases analyzed here. Instead, these cases are indicators of a broad sovereigntist endeavor to challenge the existing internet governance norms and institutions and to shape an emerging and therefore still malleable field. There is a plethora of other examples of this conflict. For instance, Russia proposed a Convention on International Information Security in 2011 (Russian Federation, 2011). Similarly, Shanghai Cooperation Organisation member states promoted a Code of Conduct for Information Security at the UNGA in 2011 and 2015 (China et al., 2011, 2015). Furthermore, China organized an annual World Internet Conference (WIC) in Wuzhen, focused on creating global internet governance norms.

However, the liberal sphere is not only challenged from outside but also from within. Particularly after the Snowden revelations in 2013, conflicts in areas such as data privacy or the domain name system have challenged the hegemonic influence of the US Government and of US companies. For instance, Brazil aimed to create a new multistakeholder forum on internet governance and hosted a first meeting in 2014. However, despite backing from other actors in the liberal sphere, the NETmundial Initiative failed. The IANA transition between 2014 and 2016, which terminated the exceptional role of the US in global Internet infrastructure, was a response to criticism of US hegemony from both liberal and sovereigntist proponents. However, these challenges do not necessarily result in a weakening of the liberal sphere. As also demonstrated by Scholte (2018) the IANA stewardship transition actually resulted in a manifestation of, e.g., the position of the US government and the (liberal) multistakeholder community. The liberal sphere adapts or even strengthens by reacting to challenges and thus prevents a fragmentation of internet governance. However, the liberal sphere suffers from two inconsistencies: (1) the weakness of political authority, and (2) domestic stability and security.

First, there is a strong reliance of the liberals on private self-regulation, soft law and discursive multistakeholder processes rather than on public international law. As a result, the liberal sphere is strong in technical authority but weak in legitimate political authority. The need for the latter is, however, increasingly felt with internet governance gaining increasing domestic political and economic importance. Particularly US technology companies have embraced a more proactive role, in some instances effectively pushing for or challenging governmental practices by positioning themselves as competing power centers or ‘Digital Switzerlands’ (Eichensehr, 2018) in the liberal sphere. Tellingly, a proposal by a private firm (Microsoft) to adopt a ‘Digital Geneva Convention’ as a classical international law treaty dealing with cyber warfare is seen with great reserve by Germany, a state which is usually a staunch supporter of multilateralism and international law. Particular developing countries

criticize these efforts to keep the dominant liberal sphere underlegalized and underinstitutionalized and thus dominated by large Western powers and large Western firms. This is also seen as a refusal of formalized specific rights and obligations, which are characteristic of the very idea of constitutionalization (Fischer-Lescano, 2016).

Second, the liberal attitude towards internet-based communication as a threat to domestic stability is changing. For a long time, the liberals have regarded this argument as a Trojan horse for strongly illiberal and undemocratic tendencies justifying internet shutdowns and censorship. Yet, for sovereigntist (and often supported by developing countries), the current configuration of norms and institutions is another instance of how a small number of Western states shapes and dominates institutions and rules with a global reach. Their core argument is that the current system for internet governance is deeply intrusive into legitimate domestic social purposes and domestic laws. Even among Western states, there is an increasing tendency to introduce legislation aimed at manifest violations of domestic criminal law, combating terrorist propaganda and disinformation, most notably when it interferes with elections, and export of dual-use technologies. The concerns of the liberal sphere in this respect sound increasingly similar to those of the sovereigntists. This weakens the liberal resistance against limitations of freedom of expression in the name of legitimate domestic concerns.

More recently, particularly the EU but also emerging powers have increasingly diverged from the current weak legalization and constitutionalization, which have raised the question whether there is a 'third way' between a 'Californian' and a 'Chinese cyberspace' as French President Macron put it during the 2018 IGF. Although it is too early to make a decisive call on this issue, we argue that it is more likely that the liberal sphere will accommodate requests for stronger internet regulation and a more proactive role of the state because this would not violate its normative core but allow the liberal sphere to remain dominant. Other liberal states, such as the US or New Zealand, are also facing increased internal contestations of their current internet policies and face public debates about, for example, hate speech, competition, data privacy, or intermediary liability (Frosio, 2018). However, conflicts within the liberal sphere are likely to increase as the current US administration has in some areas worked against this trend, for example by dismantling net neutrality rules, refusing to join the widely supported Paris Call for Trust and Security in Cyberspace, or in recent attacks on French proposals for digital taxation.

Nevertheless, the concept of spheres of authority allows for these gradual shifts in constellations of actors, policy preferences and motivations for regulation, as long as the spheres are still meaningfully distinguishable from each other. Hence, the changing shape of

spheres is not a new phenomenon. For example, early libertarian positions of internet pioneers have been abandoned once the internet became larger in scale and scope and China has remarkably expressed its support for the multistakeholder organization ICANN, despite recent efforts to subject domain name registration to governmental licensing. As argued in the previous section, security concerns are an important driver for these changing constellations of the liberal sphere. External shocks such as terrorist attacks in Christchurch increase the demand for state regulation and the liberal sphere adjusts accordingly, creating new opportunities for sovereigntist challengers to shape global internet governance debates. Hence, the conflicts over adequate internet governance institutions and norms are ongoing, transforming and unlikely to be resolved in the future.

CHAPTER 3

Illiberal norms in emergence: Russia and China as content control promoters

Daniëlle Flonk

Abstract

This paper contributes to the understanding of authoritarian states as norm entrepreneurs of content control norms. These emerging norms challenge the norm literature, which disregards illiberal norms and illiberal actors as norm entrepreneurs. This paper focuses on two distinct but coexisting strategies that Russia and China apply for promoting and developing internet governance norms. I show that these states use a combination of socialization and persuasion strategies. They employ a sequencing strategy of regional coalition-building in order to create support, after which they expand a norm's range via international organizations. These norm entrepreneurs adapt their strategies to different target groups based on the degree of internalization of the norm. This paper shows that a reassessment of norm theory in a broader context allows for extension to illiberal norms and illiberal actors, but also shows the limits since the applicability of strategies such as naming and shaming should be questioned.

I. Introduction

Content control of the internet is an emerging global norm. Whereas popular and scientific belief often assumed that the internet is an open technology, states have proven to be quite capable of controlling content (DeNardis, 2012). Accordingly, authoritarian states develop international norms on content control that challenge liberal values such as democracy and freedom of expression. The participation of authoritarian states in content control norm development is puzzling at first sight. Content control is a domestic policy domain in its essence and autocrats should not be willing to bind themselves to global norms that might constrain them. However, I argue that content control norms increase the legitimacy of authoritarian practices. Hence, this study explores the ideational factors of norm promotion by authoritarian states.

Illiberal norm development by authoritarian states remains under-researched. This is due to two biases in the norm literature. First, the literature has a liberal bias (Adamson, 2005, p. 547): whereas it is theoretically possible for norms to be illiberal, norm researchers often focus on how liberal norms diffuse, such as human rights norms (Risse-Kappen et al., 1999). Second, the literature has a directional bias (Jose & Stefes, 2018): whereas it is theoretically possible for authoritarian states to be norm entrepreneurs, norm researchers often focus on other actors such as non-state actors (Clark, 2010).

Some newer studies take these biases into account. In the norm literature, scholars have started to reassess norm promotion. For instance, Alden and Large focused on how China reframes norms on security and development (2015, also see, for instance, Bob, 2012). Similarly, the authoritarian diffusion literature has started to look at the consequences for global norms of authoritarian powers. For instance, Cameron and Orenstein find that member states of regional organizations such as the Collective Security Treaty Organizations (CSTO) are under Russian influence, leading to a decline in human rights and democracy (2012, also see, for instance, Ambrosio, 2010). Hence, in both the norm and authoritarian diffusion literature, scholars increasingly acknowledge that there is an important international dimension to authoritarianism. My research contributes to these debates by analyzing a significant case of norm promotion: Russia and China as entrepreneurs of content control norms.

I set out a norm framework that takes into consideration how institutional structures enable and constrain actors' strategies. I demonstrate two distinct but coexisting norm promotion strategies used by Russia and China. Via socialization, they include like-minded states in a regional group or organization. Via persuasion, they use reasoning to change the opinions and

attitudes of target groups. Norm entrepreneurs adapt their strategies to different institutional contexts based on the degree of internalization of the norm by the target group. Moreover, by combining socialization and persuasion, they can adopt a sequencing strategy whereby they first develop regional norms, after which they expand their range internationally. My research, therefore, addresses the biases in the norm literature and shows that causal mechanisms cannot only be applied to liberal actors, but also illiberal ones. If we want to understand changes in global governance, we have to take into account the norm promotion strategies of rising authoritarian powers.

II. Theoretical framework

II.1. Illiberal norms

Norms are shared standards of appropriate behavior for actors with a given identity (Finnemore & Sikkink, 1998, p. 891) and therefore do not prescribe a specific substance. Instead, norms are norms when they develop a sense of stickiness (Acharya, 2011, p. 106) and prescribe a sense of oughtness. Consequently, norms can be either liberal or illiberal, democratic or authoritarian. My research focuses on content control norms, in which I define content control as the process by which actors with a given identity use different technologies, policies, and justifications to influence or limit access to internet content for a given purpose.

II.2. Illiberal actors

Norms are actively built and promoted by norm entrepreneurs, which are "agents having strong notions about appropriate or desirable behavior in their community" (Finnemore & Sikkink, 1998, p. 896). They are characterized by their proactiveness; they call attention to issues or frame issues in order to align them with public understandings. Similar to norms, the concept of norm entrepreneurs does not prescribe a specific substance. These actors pursue different norms based on a variety of identities (Muller & Wunderlich, 2013, p. 37), whether they are civil society actors or authoritarian states. Therefore, my research focuses on rising authoritarian powers as promoters of content control norms.

At first sight, it might seem puzzling that authoritarian states want to promote norms on content control, which is a domestic policy domain in its essence. However, autocrats have both instrumental and ideational motivations for promoting illiberal norms. From an instrumental perspective, illiberal international norms counter the diffusion of democracy (Allison, 2008, p. 190). Notions of sovereignty and non-interference protect autocracies from unwanted interference in their regimes and prevent sanctions and demands for reform (Lindberg, 2009,

pp. 86–92). From an ideational perspective, shared international norms increase the legitimacy of authoritarian practices. They normalize content control, provide guidance on appropriate behavior, and justify authoritarian rule (Ambrosio, 2008). Hence, autocrats' motivations are also about developing norms that are an authoritative source of power (Beetham, 1991), which legitimizes authoritarian rule.

II.3. Strategies for norm promotion

Since the conceptualization of norms and norm entrepreneurs does not prescribe a specific substance of norms or actors, the empirical scope of norm research should be broadened. With regard to norm emergence, the literature focuses on two broader concepts: the agency of actors and the opportunity structures in which they operate. I, therefore, set out the strategies that norm entrepreneurs employ and the contexts in which they have to maneuver to promote new norms. I argue that these contexts themselves may also interact, providing sequencing opportunities for norm promoters.

According to the norm literature, norm entrepreneurs can use different strategies for promoting and developing new norms, such as socialization and persuasion. First, socialization refers to "the process by which the newcomer – the infant, rookie, or trainee, for example – becomes incorporated into organized patterns of interaction" (Stryker & Statham, 1985, p. 325), via education, habituation, and repetition. Norm entrepreneurs can impose social costs and pressure to influence belief and action and acculturation takes place when actors adopt the beliefs and behavior of their surrounding culture (Goodman & Jinks, 2013, pp. 4, 31). Norm entrepreneurs can use different tools for norm development via socialization, such as references to reputation, providing technical assistance and training, capacity-building, and naming and shaming (Murdie, 2014, p. 42).

Second, persuasion refers to changes in preferences via communicative action (Coleman, 2013, p. 166) and causes other actors to do or believe something by asking, arguing, or reasoning. It is a "cognitive process of information exchange and argumentation that changes minds, opinions, and attitudes about causality and effect in the absence of coercion" (Finnemore & Hollis, 2016, p. 450). A new norm becomes more legitimate once it fits more coherently with (or, is an extension of) the existing normative framework. Therefore, norm entrepreneurs can link a norm to other norms to increase its coherence, credibility, and urgency (Finnemore & Hollis, 2016, p. 451; Florini, 1996). They can also construct frames that resonate with broader public understandings of issues (Finnemore & Sikkink, 1998, p. 897) and to increase the persuasive power of arguments (Finnemore & Hollis, 2016, p. 451). One method of framing

old issues in new ways is by securitizing them. Security is a speech act (Buzan et al., 1998), whereby "(i)t is by labelling something a security issue that it becomes one" (Wæver, 2004, p. 13). When norm entrepreneurs argue that an actor is threatened in its existence, it legitimizes measures to ensure survival. They try to push policy issues towards emergency politics, where policy-making is faster, not succumbed to democratic decision-making procedures, and more means are considered appropriate. Successful securitization is therefore based on the ability of norm entrepreneurs to socially and politically construct threats (Balzacq et al., 2016, p. 495; Taureck, 2006, pp. 54–55). Hence, issues can be brought to the public agenda by framing old issues in new ways and by transforming target actors' understanding of their identities (Keck & Sikkink, 2014, p. 17).

Although socialization and persuasion are two distinctively different strategies, they do not rule out each other. On the contrary, it is not unlikely that norm entrepreneurs combine strategies to promote norms. Norms develop when actors accept persuasive messages, and repetition and socialization accelerate the internalization of a norm (Payne, 2001, p. 42). However, the strategies that norm entrepreneurs choose are dependent on the context in which they operate, such as the type of institution and their target group. In the following section, I combine these proactive strategies with the constraining and enabling features of structures. Then, I derive which promotion strategies are more likely to be employed in such a context.

II.4. Contexts of norm promotion

Although norm entrepreneurs can use different strategies for norm promotion, they also need an organizational platform from which they can act, such as regional and international organizations (Finnemore & Sikkink, 1998, p. 899). They need to find an organizational 'home' and negotiate broad support for a new norm. Like traveling salespersons, norm entrepreneurs can resort to strategic venue change (or forum shopping) when discussions about a norm do not progress sufficiently in a certain institutional context (Björkdahl, 2002, pp. 50–51; Theys & Rietig, 2020, p. 1607). Therefore, active engagement in multilateral fora is a key part of norm promotion.

The selection of different contexts for norm promotion creates trade-offs for norm entrepreneurs because the characteristics of an institutional venue influence the content of an emerging norm, but also the level of international support (Coleman, 2013, p. 170). These considerations affect the strategy of a norm entrepreneur (see Table 4 for an overview). On the one hand, choosing a limited context (e.g., a regional organization) increases the chances of successful norm development, but only has a limited reach (Finnemore & Hollis, 2016, pp.

464–467). Regional organizations are more homogeneous, consisting of a limited amount of like-minded actors that share similar values and ideas, making it more likely to find support for an emerging norm (Björkdahl, 2002, p. 133). Therefore, facing like-minded states on a local level creates opportunities for norm entrepreneurs to socialize other actors, for instance via referring to reputation, providing assistance and training, and naming and shaming. Persuasion becomes less necessary in such a limited and homogeneous context since norm entrepreneurs face less challengers. Therefore, I expect that *illiberal norm entrepreneurs are more likely to use socialization strategies in regional organizations in order to promote and develop illiberal norms.*

On the other hand, promoting norms in a global context (e.g., an international organization) increases the reach of a norm, but also leads to more disagreement and less demanding norms (Finnemore & Hollis, 2016, pp. 464–467; Stimmer & Wisken, 2019, p. 532). In other words, norm strength has a negative relationship with international support and membership (M. L. Busch, 2007, p. 758). Actors in a global context are more heterogeneous and not as like-minded as those on a regional level, and therefore have to be more actively convinced of a norm. Positions among actors are more diverse and therefore socialization becomes an ineffective strategy. When contexts are more heterogeneous, norm entrepreneurs have to employ persuasion strategies such as linking and framing norms in a way that would resonate with a broader audience. Therefore, I expect that *illiberal norm entrepreneurs are more likely to use persuasion strategies in international organizations in order to promote and develop illiberal norms.*

	Limited context (e.g., regional organization)	**Global context (e.g., international organization)**
Strength of norm	+	-
Reach of norm	-	+
Strategy	Socialization	Persuasion

Table 4. Overview of norm promotion trade-offs and strategies in different institutional contexts.

Moreover, these different contexts may interact if norm entrepreneurs adopt a sequencing strategy, whereby they develop norms first on a lower level to create basic support, after which the range of norms can be expanded horizontally (to more actors) or vertically (to more contested aspects of the norm) (Goodman & Jinks, 2013, pp. 180–182). Building winning coalitions and a critical mass is an important aspect of successful norm entrepreneurship

(Björkdahl, 2013, p. 330; Theys & Rietig, 2020, p. 1608). Norm entrepreneurs evaluate which venue will increase strong support for a weak norm and less widespread support for a strong norm (Coleman, 2013, pp. 171–172). When considering this trade-off, norm entrepreneurs can strategically sequence norm promotion in limited and global contexts. They first build coalitions by socializing like-minded states in regional organizations, after which they persuade less like-minded states in international organizations. Therefore, I expect that *illiberal norm entrepreneurs combine socialization strategies in regional organizations, and persuasion strategies in international organizations in order to promote and develop illiberal norms*.

III. Case background

III.1. Content control norms

In order to assess the strategies of illiberal norm entrepreneurs for promoting illiberal norms, I look at how Russia and China promote content control norms in regional and international institutions. Content control norms can vary from taking into account human rights and an open internet on one extreme to a state-led internet on the other extreme. For instance, governments filter or block webpages for purposes such as protecting children, preventing terrorism, or censoring the opposition. They make new laws or use existing ones to curb hate speech, slander, or defamation online. Or they surveil and use counter-information campaigns in order to intimidate or overwhelm opponents such as cybercriminals, demonstrators, or journalists (Deibert et al., 2010, p. 7). Hence, content control is not a dichotomy but a concept on which the conception of appropriate control varies between actors. Varying conceptions exist on what type of content should be regulated, to what extent this content should be regulated, and what regulatory tools should be used. Consequentially, content control norms can also be consistent with illiberal or authoritarian principles.

Russia and China promote illiberal content control norms via the concept of information security. Information security norms are a Trojan horse for increased content control (Ebert & Maurer, 2013, p. 1055). There are three dimensions to the logic of information security. First, it is defined broadly, since it entails "the status of individuals, society and the state and their interests when they are protected from threats, destructive and other negative impacts in the information space" (SCO, 2009, p. 9), with a threat including any information that is harmful to social, political and economic systems. Second, Russia and China try to reorder the internet via content regulation and censorship, whereby states are the core actors that should keep order in cyberspace (Maréchal, 2017, p. 35). Third, they argue that global cyberspace should be governed by an intergovernmental model under UN institutions, which are labeled as

democratic since they are based on the principle of 'one country, one vote' (Mueller, 2011, p. 181).

The push for information security norms is part of a larger conflict about the openness of the internet, fought out between an illiberal sphere (led by Russia and China) and a liberal sphere of authority (led by US and EU member states) (Flonk et al., 2020).[2] For instance, in 2011, Russia proposed the creation of the UN Group of Governmental Experts on Information Security (UNGGE) that focused on establishing norms in internet governance. In 2018, Russia proposed the establishment of an Open-Ended Working Group that has a broader membership than the UNGGE, competing with a US resolution on a continuation of the UNGGE. The illiberal sphere of authority has not been unsuccessful in establishing new content control norms, for instance by adopting a new International Telecommunication Union (ITU) treaty in 2012 (ITU, 2012b). Whereas the liberal sphere was reluctant to regulate content for a long time, it seems that the tide is turning. Policymakers in the US and EU are increasingly skeptical of private internet governance (Farrell & Newman, 2021), and calls for countering terrorist content and disinformation are increasing, such as the Paris Call for Trust and Security in Cyberspace and the Christchurch Call. Hence, the illiberal sphere is continuing the promotion of illiberal norms (and sometimes succeeds in doing so) and the liberal sphere is moving towards more regulation and a more important role for states in content control.

III.2. Russia and China as norm entrepreneurs

I look at the case of Russia and China as entrepreneurs of content control norms for two reasons. First, is an example of the promotion of illiberal norms. Second, it is an instance of authoritarian states as norm entrepreneurs. Hence, I assess how Russia and China promote information security norms in several regional and international institutions. These regional institutions include the BRICS, the CSTO[3] and the Shanghai Cooperation Organisation (SCO),[4] and the international institutions include the United Nations (UN)[5] and the World Internet Conference

[2] Countries in the liberal sphere favor limited content control and a freer flow of information. They oppose a multilateral form of global internet governance under the UN and instead, favor multistakeholder models that include non-state actors.
[3] The CSTO was established in 1994 and current (full) member states are Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia, and Tajikistan.
[4] The SCO is an intergovernmental international organization created in 2001 by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan and focuses on increasing mutual trust and cooperation between these countries. In 2017, India and Pakistan became member states.
[5] A number of UN agencies, fora and groups responsible for internet governance are the Internet Governance Forum (IGF), the International Telecommunication Union (ITU), the United Nations Educational, Scientific and Cultural Organization (UNESCO) and the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE).

(WIC).[6] The regional organizations have varying degrees of membership homogeneity (with BRICS being the most diverse), but nonetheless a higher authoritarian homogeneity than the UN and the WIC, where more democratic actors participate. This selection enables the assessment of the strategies that Russia and China employ in varying institutional contexts and aimed at different target groups.

Russia and China are also different in two ways. First, Russia has a more decentralized internet infrastructure than China. Therefore, Russia is relatively more dependent on legislation than on technical capabilities for controlling content (Stadnik, 2021). Second, Russia is an electoral autocracy and China is a closed autocracy. Hence, of the two states, China is a least likely case for information security norm promotion. Nevertheless, Russia and China are still similar in two important ways, making them relevant cases for my research. First, they take a similar stance on content control and actively promote illiberal norms accordingly. Second, they do so in different regional and international organizations.

III.3. Sources and operationalization

I look at the different strategies that Russia and China employ by using content analysis. I adopt a discursive approach whereby I assess how these norm entrepreneurs construct and develop content control norms over time. Since this discourse is aimed at different target audiences in different regional and international organizations, I expect variation in norm promotion strategies.

I selected a variety of sources, ranging from official statements (such as interviews and statements) to official publications (such as position papers and reports) to legal publications (such as agreements and resolutions). Speech actors included state actors (Russia and China) and international organizations (BRICS, CSTO,[7] SCO, UN, and WIC).[8] I selected these sources via the national governments' and institutions' websites[9] based on references to information security, internet governance, digital governance, and content regulation. I used secondary literature to identify additional sources. When sources referred to (1) the promotion of information security norms (2) in the context of regional or international organizations, I

[6] The WIC is a yearly internet governance event organized by China focused on the development of global internet governance norms.
[7] CSTO documents were collected and coded in the Russian language with the help of a student assistant.
[8] I allowed for statements by regional and international organizations to get an indication of the extent of internalization of the norm and dominant frames.
[9] The main websites used for data collection were: https://digitallibrary.un.org/; https://en.odkb-csto.org/; http://eng.sectsco.org/; https://www.fmprc.gov.cn/mfa_eng/; https://infobrics.org/; https://www.mid.ru/en/main_en.

included them in the analysis. In total, 152 documents were analyzed (of which 50 had a clear international context and 94 had a clear regional context), spanning from 2009 until 2019.

After collecting the relevant sources, I coded segments in those documents that indicate the use of socialization and persuasion strategies. Socialization strategies are operationalized by measuring when norm entrepreneurs refer to capacity-building, confidence-building measures, exchange of expertise, consensus, harmonization of legislation, the importance of regional cooperation, increased cooperation, joint actions, naming and shaming, norm-conforming behavior, technical assistance, and reputation. Persuasion strategies are measured when norm entrepreneurs use argumentation to convince other actors by trying to increase the effectiveness and credibility of arguments; framing arguments in a certain way (e.g., by using security frames); by linking norms to other norms (e.g., sovereignty) and principles (e.g., development). Furthermore, I coded instances of combining strategies, namely international norm building by regional organizations, and sequencing regional and international cooperation. One segment could have multiple codes. In total, 2,533 segments were coded. Besides these discursive strategies, I coded for each source the title, date, speech actor, organization, context (regional or global), and document type.

I coded the publications and statements using MAXDQA (Plus 2020, release 20.4.0) until the analysis saturated and no new instances of norm promotion strategies could be found. Hence, whereas not the whole population of discourse can be analyzed, the sample of documents is representative of the discourse across regional and international institutions over a ten-year period. The complete MAXQDA database is available upon request. Finally, I use the proposals for a Code of Conduct for Information Security in 2011 and 2015 as an illustrative case study to show the sequencing strategies of Russia and China.

IV. Analysis

The analysis consists of four parts. In the first part, I give a brief overview of the distribution of persuasion and socialization strategies across regional and international organizations. In the second part, I assess the socialization strategies that Russia and China employ in regional organizations. In the third part, I set out the persuasion strategies that they use in international organizations. In the fourth and final part, I explain how Russia and China combine these strategies in different institutional contexts.

IV.1. Distribution of socialization and persuasion strategies

In Table 5, I show the distribution of persuasion and socialization segments found in regional and international organizations. By eyeballing this data of coded segments, there is a strong indication that Russia and China are more likely to use socialization strategies in regional organizations and persuasion strategies in international organizations. For instance, in the CSTO about 63% of the discourse found was part of a socialization strategy, whereas this was only 20% at the UN. Hence, the homogeneity of the organization affects norm promotion strategies. This is also underlined by the differences between regional organizations, whereby most socialization strategies (63%) were found in the CSTO, which is the most homogeneous organization. In the SCO, about 43% of the strategies were based on socialization, which could be explained by its larger and more diverse membership. 42% of the strategies in the BRICS were based on socialization, which could be explained by its more heterogeneous character. Furthermore, persuasion strategies do not remain absent from regional organizations since China and Russia also apply frames and link norms in such a context. The number of segments gives a first indication of the different strategies used in different institutional contexts. In the following parts, I set out these socialization and persuasion strategies in more detail.

	CSTO	**SCO**	**BRICS**	**UN**	**WIC**
Socialization	290 (63%)	159 (43%)	49 (42%)	120 (20%)	22 (20%)
Persuasion	172 (37%)	214 (57%)	67 (58%)	492 (80%)	89 (80%)

Table 5. Overview of total number and percentages of socialization and persuasion strategy segments coded in different institutional contexts.

IV.2. Socialization

On a regional level, Russia and China often face already like-minded states and therefore employ socialization strategies for norm promotion. This has three implications for the causal mechanism of norm promotion. First, Russia and China socialize like-minded states by including them into a regional group via raising their status and reputation, and praising norm-conforming behavior. Second, they improve their relationships by exchanging expertise, providing technical assistance, and working on capacity-building. Third, these socialization mechanisms lead to a taken for grantedness among actors whereby the norm is no longer questioned and expressed collectively. In turn, it enables a more effective norm entrepreneurial strategy on the international level.

First, Russia and China socialize other states into regional organizations to gain support for content control norms. China hereby focuses mainly on the SCO and Russia on the CSTO.

One strategy is trying to raise the status and reputation of target countries. For instance, Russian Foreign Minister Sergey Lavrov said that Russia attached great importance to joint work on information security at different fora such as the SCO (Russia, 2014a). President Xi Jinping stated that information security cooperation demonstrated "the strong vitality of the SCO", constituting a solid foundation for future growth of the organization (China, 2014b). Norm entrepreneurs refer to target countries as companions. For example, Chairman of the Federation Council, Sergey Mironov stated that information security is an essential component of the CSTO security capabilities of Russia and its allies. Due to informational provocations against Russia and their 'friends', policy coordination is important (CSTO, 2011). Similarly, Russia referred to other BRICS countries as partners in developing information security norms (Russia, 2017). Another way of socializing target groups is by complimenting member states' (compliant) behavior toward information security. For instance, Sergey Lavrov stated that SCO member states are effectively standing up against information security threats (Russia, 2015a). Hence, norm entrepreneurs include target countries into a community with a common purpose, namely the development of content control norms.

Interestingly, I found no evidence for naming and shaming strategies, whereas the literature would expect this to occur. I argue that naming and shaming is not a relevant mechanism in the context of illiberal actors promoting illiberal norms for three reasons. First, states cannot easily address other states' illiberal behavior, because there are severe diplomatic and reputational costs involved (whereas the costs for non-state actors are lower). Additionally, it is difficult to shame actors for liberal and feel-good behavior. Finally, by naming and shaming other actors for liberal and feel-good behavior, a state would admit that they were acting in illiberal ways themselves. Hence, although naming and shaming might be relevant in the context of certain feel-good norms, these strategies remained absent in my analysis, underlining the liberal and directional biases of the norm literature addressed in the introduction.

Second, via different regional constellations, information security cooperation occurs by exchanging expertise, providing technical assistance, and joint actions. Russia and China exchange intelligence between relevant authorities and organize scientific and practical events to strengthen information security (Russia, 2015a). For instance, one of the areas of SCO cooperation is "exchanging experience, training of specialists, holding working meetings, conferences, seminars and other forums" (SCO, 2009). With regard to countering terrorism, SCO member states cooperate in the Regional Anti-Terrorist Structure (RATS) to collect and analyze data, maintaining a databank on terrorist, separatist and extremist actors, and conduct operational and technical exercises (SCO, 2002, pp. 3–4). Likewise, since 2009, the CSTO is

carrying out joint operations in operation PROKSI,[10] which is focused on countering information crimes, and suppressing information resources in member states. In operation PROKSI, Russia provides practical assistance to law enforcement agencies, exchanges expertise on combatting cybercrime, and assists in the development of specialized units (CSTO, 2009). Furthermore, the CSTO established a Center for Modern Information Technologies in Russia for information security training, exchanging experience, and recruiting and preparing information security specialists (CSTO, 2012). In the BRICS, there is also cooperation in the area of information security by sharing information and best practices, implementing policy coordination against cybercrime, and joint research and capacity-building (BRICS, 2015). Hence, these regional organizations are increasingly investing in coordinated information policy. According to CSTO Secretary General Nikolai Bordyuzha, these collective information security systems contribute to the consistent development of cooperation, exchange of views and expertise, and dialogue between members (CSTO, 2013c).

Third, since Russia and China socialize states on a regional level, information security norms are often so well-developed that their substance is no longer challenged. Member states of the BRICS, the CSTO, and the SCO often take a common stance on content control. For instance, SCO member states stated that one of the priority areas for cooperation is combatting modern information technology crimes (SCO, 2016a). The SCO heads of state agreed that "(t)he member states will encourage building a peaceful, secure, fair and open information space based on the principles of respect for state sovereignty and non-interference in the internal affairs of others" (SCO, 2012a). Furthermore, member states praised the work of the RATS in coordinating information security activities of the member states (SCO, 2016b) and appreciated joint anti-cyberterrorism exercises (SCO, 2018). Similarly, Nikolai Bordyuzha stated that information security has become an integral element of the CSTO collective security system (CSTO, 2013c). Hence, there is a consensus that the internet should not propagate terrorism, extremist and separatist ideologies (SCO, 2012a) and that formulating proposals at the UN level is important (SCO, 2012b). There is also an attempt to improve and harmonize national legislation of the member states (CSTO, 2014) and to develop common legal frameworks for information security (CSTO, 2013b; SCO, 2013). Within the BRICS, the focus is less on the substance of the norm and more on the willingness to develop an intergovernmental global internet governance system, especially under UN auspices (see, for instance, BRICS, 2014, article 48-50, 2015, article 34).

[10] In Russian: Противодействие криминалу в информационной среде (ПРОКСИ), i.e., countering crime in the information sphere.

Member states do not only take a common stance on information security norms but also act accordingly. The participation in joint operations and exchange of best practices show that member states successfully control content. According to the director of the SCO RATS Executive Committee, Zhang Xinfeng, SCO member states share intelligence and carry out exercises to raise the information security capabilities of member states (Global Times, 2014). For instance, in 2017, the SCO member states held a joint anti-cyber terrorism exercise in China, "aimed at curbing the use of the internet for terrorist, separatist and extremist purposes." (SCO, 2018) Similarly, regular joint PROKSI operations identify thousands of internet sources that disseminate information that causes political damage, which leads to criminal cases against persons involved in their creation and maintenance (CSTO, 2016). Hence, to a great extent, information security norms are internalized on a regional level. As a consequence, Russia and China have strong regional coalitions and support for the promotion of content control norms on an international level, which will be addressed in the third part of the analysis.

IV.3. Persuasion

On an international level, Russia and China face more diverse target groups. Hence, they change strategies dependent on the internalization of the norm by the target group and thereby sometimes have to employ persuasion strategies for norm promotion. This has three implications for the norm promotion process in a global context. First, non-likeminded target groups in international organizations have to be convinced of the validity of arguments and persuaded into supporting new norms. Second, in order to make a convincing argument, Russia and China often use security frames in the field of content control and internet governance. Third, these frames resonate with a broader and liberal audience and circumvent problematic hurdles such as a direct challenge of online freedom of expression.

First, it is evident that it is unlikely that China and Russia will socialize countries like the US and EU member states into supporting content control norms since they limit online freedom of expression. Hence, in broader institutional contexts such as international organizations, they have to employ persuasion to convince non-likeminded states of the necessity of content control norms. Since they face less like-minded states in a heterogeneous global context, Russia and China change their discourse. Whereas norms as fighting separatism and extremism are emphasized on a regional level, China and Russia transform these arguments to show the necessity of global content control norms without illustrating their specific interpretation.

Second, in order to show the necessity of global content control norms, Russia and China securitize content. Since content control norms are not a dichotomy but a continuum on which the degree of control can vary, there are many gray areas where content control might be seen as legitimate. For instance, cyberterrorism and cybercrime are seen as legitimate reasons for controlling internet content by western states (for instance, Council of the European Union, 2017). These gray areas create opportunities for Russia and China because they provide a common ground for developing norms. Cybercrime and cyberterrorism relate to existential threats experienced by all members of the international community and are therefore used to mobilize support for content control norms.

In international organizations, often occurring security frames are cybercrime, cyberterrorism, international security, and cyberwarfare. For instance, according to the Chinese submission to the OEWG, "(s)urging cyber attacks and cyber crimes, as well as cyber terrorism as a global menace (…) Terrorist groups' use of the Internet for promotion and incitement, recruitment, and plan and coordination of attacks is the major source of the current terrorist activities, and jeopardize the security and stability of all states." (China, 2019) At the WIC, President Xi Jinping stated that "(c)yber surveillance, cyber attack and cyber terrorism have become a global scourge" and therefore the international community has to increase cooperation (China, 2015b). According to the Chinese Minister of Foreign Affairs, Wang Yi, the international community should "crack down hard and effectively on the use of the Internet and other new means of communication by terrorists to instigate, recruit, finance or plot terrorist attacks" (China, 2014c, also see, for instance, Russia, 2015b). Hence, in an international context, information security is framed in a specific way; one that relates to existential threats and security risks experienced by target countries.

In regional organizations, norm entrepreneurs also use security frames but much broader ones. When targeting more like-minded states, Russia and China emphasize fighting "the three evils" of terrorism, extremism, and separatism (SCO, 2018), the prevention of protest and uprisings, and protecting (broadly defined) national security. For instance, Chinese Public Security Minister Guo Shengkun stated that the SCO had shared concerns about information aimed at overthrowing the authorities and provoking a new wave of color revolutions (The Moscow Times, 2014, for similar concerns in the CSTO, see, for instance, CSTO, 2018). Nikolai Bordyuzha also referred to the dangers of revolutions: "How did the Arab Spring begin? With the information impact on the population." (CSTO, 2013a) Hence, information as a threat is defined in a broad way that undermines the political, economic, and social security of states (SCO, 2013, 2014a). This includes aspects such as the spread of radical and extremist ideas

(Russia, 2015a), creating an atmosphere of fear and panic in society (SCO, 2009), and stirring up social unrest (China, 2014b).

Third, the securitization of content resonates with a broader audience. Promoting content control directly would lead to criticism by countries as the US and EU member states. Norm entrepreneurs on the one hand and less like-minded states on the other, deal with alternative perceptions of appropriateness. However, securitizing content is a way to circumvent these challenges. In other words, Russia and China try to fit content control more into the existing framework of acceptable norms. They transform security frames to show the necessity of global content control norms without illustrating their specific domestic or regional interpretations. Even though some actors might be extra critical of broad uses of concepts as information security, enabling that content control norms may mean different things in different contexts might actually increase their chance of diffusing. Since information security is an ambiguous concept, it can fit within different contexts and interpretations. Hence, norm entrepreneurs use argumentation and reasoning and at the same time leave room for regional interpretations of the norm.

IV.4. Combination

So far, it is clear that Russia and China use socialization strategies towards like-minded states and try to convince non-likeminded states via persuasion strategies. Hence, norm entrepreneurial strategies are adapted to different institutional contexts based on the degree of internalization of the norm by the target group. In a way, Russia and China are traveling salespersons that change regional and international venues and adapt their norm-selling techniques to these contexts. Russia labeled this approach multidimensional cooperation, which it views "(…) as an important factor for making the UN more efficient. We intend to direct our efforts within the UN towards further enhancing cooperation with the CIS countries, CSTO and the SCO members, and coming up with common approaches within BRICS" (Russia, 2015b). Similarly, in order to broaden international dialogue, China stated that it focuses on regional organizations such as the SCO on the one hand, and international organizations such as the UN on the other (Organizing Committee for the WIC, 2016).

Moreover, Russia and China adopt a sequencing strategy of building regional coalitions and consequentially promoting norms in a heterogeneous global context. For instance, Russia intends to use the BRICS for "launching initiatives" in the area of international information security (Russia, 2013). The country also stated that it has repeatedly introduced proposals to the UNGGE in cooperation with BRICS and other states (Russia, 2017). Similarly, SCO

member states agreed to coordinate their positions on information security and internet governance within the UN and other fora (SCO, 2014b, 2017). Hence, norm entrepreneurs try to build coalitions on a regional level where members are easier to socialize and norms are more likely to be internalized. After they built a critical mass in a regional context, they negotiate broader support on an international level.

A prime example of a sequencing approach is the promotion of the Code of Conduct for Information Security. In 2011, four SCO member states (China, Russia, Tajikistan, and Uzbekistan) proposed this Code of Conduct to the UN General Assembly. The Code of Conduct calls on states to cooperate on the restriction of the distribution of information relating to terrorism, secessionism or extremism, or undermining other countries' political, economic and social stability (China et al., 2011). Hence, it defines information security broadly, in line with Russia and China's conceptions of content control norms. The Code of Conduct did not get global backing in 2011. However, content control norms gained more support at a regional level and the SCO member states considered it important to continue efforts aimed at co-authoring a new version of the Code of Conduct (SCO, 2015). In 2015, all six SCO member states (namely China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan) submitted a revised version to the General Assembly (China et al., 2015). According to China, achieving a consensus on international norms is necessary and in the security interest of all countries (China, 2014a), "given the frequent incidents in cyberspace." (China, 2015a) According to Ministry of Foreign Affairs Spokesperson Alexander Lukashevich, the objective of the Code of Conduct is "to define the rules of responsible behavior by states in the light of emerging cyber threats and challenges of a military-political, terrorist and criminal nature." (Russia, 2011) The reference to security interests shows how norm entrepreneurs try to securitize content in a heterogeneous global context.

The revised Code of Conduct did not contain many changes and was again not supported by all UN member states. Nevertheless, the two codes are noted in several UNGGE reports, acknowledging the norm development efforts by the SCO (UNGA, 2013, p. 8, 2015a, p. 7). This case illustrates how Russia and China are building coalitions with like-minded states on a regional level and use these coalitions to promote content control norms on an international level. SCO member states work together at the UN to promote international information security norms (Russia, 2015a). Hence, regional cooperation not only improves national information security but also strengthens international norm promotion activities.

V. Conclusion

In this paper, I demonstrated the development of content control norms by Russia and China. Rising authoritarian powers use socialization and persuasion strategies to promote norms. Socialization takes place when Russia and China face like-minded states in regional organizations: they praise norm-conforming behavior, raise the status of target groups, and exchange expertise. Persuasion takes place when norm entrepreneurs face less like-minded actors in international organizations: they use argumentation to convince others, such as security frames. These findings show that norm entrepreneurial behavior depends on the homogeneity of their context. Moreover, the differentiation of context enables sequencing strategies whereby norm entrepreneurs first develop regional norms, after which they expand their range internationally (Goodman & Jinks, 2013, pp. 180–182).

The findings show that there is an important international dimension to authoritarianism (Tansey, 2016, p. 3; Von Soest, 2015, p. 625). Authoritarian states promote content control norms actively, consistently, and over time. They are normative challengers who try to change global internet governance. Hence, my causal framework based on norm theory applies to both liberal and illiberal actors.

The findings also indicate that securitization is increasingly important in the development of content control norms. By using security frames, norm entrepreneurs push internet content into the realm of governance. It functions as a way of finding common ground among less like-minded states, such as democracies and autocracies. To a certain extent, these efforts are successful. For instance, actors within the liberal sphere are increasingly leaning towards more regulation of harmful and terrorist content (Kierkegaard, 2007).

This research also has limitations. First, with regard to norm theory, I found no instances of naming and shaming strategies. This does not mean that norm theory is not useful, since the general framework is still applicable to illiberal actors. It does mean that the scope conditions of norm development might vary between different types of norms and different types of actors. Naming and shaming are problematic with regard to authoritarian practices and actors, which brings to light a selection bias in the norm literature.

Second, I did not address incentive-based strategies as alternative explanations. Norm entrepreneurs can employ material resources such as positive inducements (e.g., trade arrangements) and coercion (e.g., sanctions) (Finnemore & Hollis, 2016, p. 449). For instance, China's Digital Silk Road aims to improve communication infrastructure in developing countries, which provides target countries more means for internet content regulation and

censorship (Patrick & Feng, 2018). However, collecting direct evidence of incentive-based strategies is problematic and not within the scope of this article. Most importantly, I showed that rising authoritarian power strategies are not only about power politics (in line with, for instance, Ho, 2020) and that there are important ideational factors to authoritarian norm promotion.

My study opens up new avenues for both norm and internet governance research. First, with regard to norm promotion strategies, my research compared strategies between regional and international organizations. However, future research could assess within-organization variation over time, for instance by assessing whether norm entrepreneurs adapt their strategies when regional organizations become more heterogeneous. Second, with regard to norm entrepreneurs, I found some indication that China and Russia align and boost each other's norm promotion efforts. In 2014, during a Russian-Chinese consultation on information security, the countries "reaffirmed that their approaches on these issues are strategically close" and agreed to enhance cooperation at different regional and international organizations (Russia, 2014b). Coordination between illiberal norm entrepreneurs is an interesting avenue for future research. Finally, the shift to a securitized and more regulated internet is a significant countermovement in internet governance. To analyze these developments, internet governance should be tied in more with international relations theory. Alternative internet governance models are emerging, and we should not overlook the shifting discourses that go with them.

CHAPTER 4

Why governments control content: Comparing content removal requests between regimes

Daniëlle Flonk

Abstract

In this paper, I link the removal of internet content to regime type. I differentiate between different types of content: political and security content. Demand for controlling political content is higher in autocracies than in democracies, they have fewer constraints, but more alternatives for requesting intermediaries to remove content for them. With regard to security content, demand for controlling security is higher in democracies, they are not more or less constrained and they have fewer alternatives for requesting intermediaries. Hence, the effect of regime type on content control is conditional on the type of content targeted. In order to test this argument, I estimate a negative binomial hurdle model using evidence from Google transparency reports. I find that although democracies control less political content than autocracies, liberal democracies are more likely to control security content than closed autocracies. This means that framing content as security-related would enable its censorship in democracies. By distinguishing between content types, this paper provides a more complete picture of content control and underlines that democratic regimes also control internet content.

I. Introduction

In order to deal with the increasing scope of the internet, states try to control its content. One way is removing this content and states rely on intermediaries to do so. Internet intermediaries are "third party platforms that provide mediation between Internet content and the humans who provide and access this content" (DeNardis, 2012, p. 725). Hence, they do not create content but facilitate transactions among those who produce and access content (DeNardis, 2012, p. 726). They constitute points of control (Zittrain, 2003) for monitoring, filtering and blocking content (Birnhack & Elkin-Koren, 2003, p. 4; Elkin-Koren & Haber, 2016, p. 113). Since online service providers such as Google, Facebook, and Twitter manage content on their platforms, governments submit removal requests to these private companies if they want this content to be deleted. Hence, it is not only intermediaries that control internet content, but also states that request or pressure companies to do so. This paper analyzes content removal requests by governments and the reasons for these requests.

This research is embedded in the broader internet governance literature debates in two ways. First, instead of conceptualizing the internet as a liberation technology democratizing authoritarian states (see, for instance, Diamond, 2010; Diamond & Plattner, 2012; Krueger, 2006; Postmes & Brunsting, 2002), the internet governance literature has started to acknowledge that the internet can challenge human rights around the world (see, for instance, Golkar, 2011; Rød & Weidmann, 2015; Stoycheff et al., 2018; Tucker et al., 2017). Second, content regulation was for a considerable time in public perception and the academic debate solely linked with authoritarian control (see, for instance, Boas, 2006; Deibert et al., 2008, 2010; Gomez, n.d.; Hellmeier, 2016; Kalathil & Boas, 2003; Kerr, 2014, pp. 33–34; King et al., 2013a; K. E. Pearce & Kendzior, 2012; Rodan, 1998; Wacker, 2003). When the OpenNet Initiative investigated liberal democracies in 2012, they found no evidence for content filtering (2012) and Dick et al. argued that "(g)overnment control of the Internet cuts out the very heart of its democratic ambitions." (Dick et al., 2012, p. 7)

Recently, academics have started to recognize that distinctions between democracies and autocracies are not so clear-cut (A. Busch et al., 2018, p. 13). All regimes face challenges concerning internet content (Hintz & Milan, 2018b, p. 3951) and authoritarian and illiberal practices with regard to access to information and freedom of speech online are also present in democracies. Authoritarian practices "sabotage accountability and thereby threaten democratic processes" and illiberal practices "infringe on the autonomy and dignity of the person, and they are a human rights problem" (Michaelsen & Glasius, 2018, p. 3789).

In the content control literature, two separate research tracks on the role of authoritarian and democratic regimes exist. Sufficient attention has been given to internet censorship in authoritarian regimes. For instance, Boas poses that authoritarian states can effectively control content while still promoting internet development (2006). Roberts argues that even circumventable censorship has an impact on access to information for individuals and is, therefore, a useful strategy in authoritarian regimes (2018, p. 4). King, Pan and Roberts state that China's censorship program is mainly aimed at curtailing collective action by silencing comments aimed at social mobilization (2013a).

Other scholars acknowledge that content control also occurs in democratic regimes (for instance, Deibert et al., 2010; Deibert & Rohozinski, 2010; Yangyue, 2014), and have recently started to explore these illiberal and authoritarian internet governance practices. For instance, Hintz and Milan argue that surveillance in western democracies is institutionalized because it is in line with governmental practices and popular demand (2018b). Bak et al. research the role of the internet in state repression and find that the internet can also function as a shield for citizens in democracies, especially when the executive is constrained (2018). Meserve & Pemstein made a first step to shedding a light on the causal mechanisms behind content control behavior of democracies (2018). They use data from Google transparency reports to analyze the content removal requests that governments submit to the platform. They argue that even democratic states request for content removal:

"(...) in response to demands to restrict speech, either to influence public opinion, reduce criticism of public officials, limit citizens' access to media, and other sources of information, or, more benevolently, to bolster national security or protect individuals' reputations or privacy" (Meserve & Pemstein, 2018, p. 246).

In other words, democracies also control content online in response to criticism or unrest. The authors argue that political motivations for content control become important in situations of internal dissent; when there are riots, protests, and terrorism, democratic politicians have incentives to push back against opposition and they can legitimize limitations to freedom of speech (Meserve & Pemstein, 2018, pp. 246–248).

However, it remains unclear what the content control differences are between democracies and autocracies. Hence, in order to synthesize these separate research tracks on authoritarian and democratic regimes, I compare regime types to see to what extent our assumptions about different regime types hold. A broad and structural assessment across states remains a blind spot in the field of content control and there is little comparative empirical

evidence about under which circumstances states censor the internet (Breindl, 2013, p. 36). Hence, assessing the content control practices of democracies and autocracies can provide new insights into the causal mechanisms and dynamics of content control.

In the literature on political regimes, there is the (often implicit) assumption that democracies are more accountable and therefore have a lower likelihood of repression (Davenport, 2007b, p. 10; see, for instance, Davenport & Armstrong, 2004; De Mesquita et al., 2005; Fein, 1995; Keith, 2002; Regan & Henderson, 2002). However, according to domestic democratic peace theory, there is a differential impact of regime type on repression (Davenport, 2004, 2007b). For instance, Davenport acknowledges that democratic political institutions only limit certain aspects of repression and therefore argues that researchers should distinguish between types of coercive behavior (2007b, pp. 11–12). Furthermore, democratic institutions are only able to limit repression within certain contexts. In situations of political conflict, even democracies can resort to repressive behavior to eliminate challengers (Davenport, 2007b, pp. 14–15) and security threats might push democracies towards more coercive behavior. In other words, democracy plays an important role in decreasing state repressive behavior, but it is conditional (Davenport, 2007b, p. 9).

A growing literature relates to this call for the differential impact of regime type. For instance, Von Soest and Grauvogel show that closed autocracies rely on identity-based legitimacy claims, whereas electoral autocracies rely on adequate procedures, thereby mimicking democracies (2017). Conrad et al. argue that electoral contestation is related to more government abuse that leaves scarring on a victim's body, and leaders in states with powerful courts are more likely to employ clean torture (2018). This paper contributes to this small but growing differential impact debate in two ways. First, I show the importance of distinguishing between different types of coercive behavior by focusing on the control of different types of content. I argue that repressive behavior in the context of internet governance is conditional on the type of content targeted. Second, I show that democratic political institutions decrease specific forms of repression only within certain contexts. Demands for, constraints of, and alternatives to content control vary between regime types and, as a consequence, control of content related to security threats is even more prominent in democracies than in autocracies. Therefore, I differentiate between regime types and assess how they affect the reasons for content control.

To take on this endeavor, I conduct a comprehensive analysis of content control behavior of states using transparency report data from Google. Instead of conducting small-N qualitative analysis (see, for instance, Bambauer, 2009a; Breindl & Kuellmer, 2013; Golkar,

2011; King et al., 2013a; Roberts, 2018; Ververis et al., 2020; Wagner, 2014; J. Wright & Breindl, 2013), content control data derived from Google transparency reports allows us to move into the field of broader comparison. This data has great added value because (1) content control data is hard to come by, (2) it is comparable between states, and (3) it has a broad reach to all countries in the world. Hence, this data provides a unique opportunity to measure and compare content control practices across regime types. Using this novel data, I assess the causal mechanisms behind the relationship between regime type and different types of content control.

I differentiate between different types of content: political and security content.[11] Political content refers to content that "express(es) views in opposition to those of the current government" (OpenNet Initiative, n.d.), such as speech that criticizes the government and political leaders, or upsets the public order. I argue that demand for controlling such content is higher in autocracies than in democracies, that autocracies have fewer constraints, but more alternatives for requesting intermediaries to remove content for them. Security content refers to content "related to armed conflicts, border disputes, separatist movements, and military groups" (OpenNet Initiative, n.d.), such as terrorist and extremist content. I argue that demand for controlling security content is often higher in democracies, that democracies are not more constrained and they have fewer alternatives for requesting intermediaries. Hence, the effect of regime type on content control is conditional on the type of content targeted. My study shows that in the field of content control, it is paramount to distinguish who controls what content for which purpose.

II. Theory

II.1. Content control

I define content control as the process by which actors with a given identity use different techniques, policies, and justifications to influence or limit access to internet content for a given purpose. Content control norms and policies can vary from taking into account human rights and an open internet on one extreme to a state-led and closed internet on the other extreme. Controlling content to some extent is seen as necessary or even desirable, depending on the social norms in a specific jurisdiction, for instance, content on child abuse material, hate speech, and copyright infringements. However, it can also be an illiberal practice, for instance when it limits political speech or when there is a surveillance culture (Hintz & Milan, 2018b), leading

[11] There are other types of content, such as social content, content related to the information economy, hate speech, and the protection of youth and minors. Although it is not within the scope of this paper to analyze this large variety of content types, I address them briefly in the conclusion.

to prosecution and chilling effects. Hence, content control is not a dichotomous concept (Bambauer, 2009b, p. 6), but has several dimensions on which the conception of appropriate control varies between actors with a given identity. For instance, different conceptions exist on what type of content should be regulated, to what extent this content should be regulated, and what regulatory tools should be used for this purpose. The distinction between different types of content, its purposes, and the actors involved in its governance is important for explaining the control of that content. There is a need to take on a more differentiated perspective on authoritarian internet practices, taking into account a diversity of practices and norms across countries (Hintz & Milan, 2018b, p. 3952). In order to take on this endeavor, I differentiate between two types of content: political content and security content.

Political content refers to content that "express(es) views in opposition to those of the current government" (OpenNet Initiative, n.d.). Hence, it is content related to First Amendment-type rights, which include the freedom of speech, assembly, travel, and press; the freedom of association and belief without appraisal or investigation; and the freedom to boycott or strike without suffering penalties (Davenport, 2007a, p. 2; Goldstein, 2001, pp. xxx–xxxi). Many states criminalize speech that criticizes the government and political leaders. For instance, in Brazil in 2012, the head of Google Brazil was arrested for not removing YouTube videos targeting political candidates. In Turkey, content criticizing Mustafa Kemal Atatürk and the burning of the Turkish flag is criminalized. In Vietnam, antigovernment content is controlled and in Thailand, criticism of the royal family is prohibited. Political content also includes the prohibition of content that upsets the public order. For instance, countries such as Kuwait and Lebanon have laws that prohibit the disruption of this public order. Hence, this type of content control result in a limitation of press freedom and amateur speech online (Gillespie, 2018, p. 38).

Security content refers to content "related to armed conflicts, border disputes, separatist movements, and military groups" (OpenNet Initiative, n.d.), of which content related to terrorism and extremist is most prominent. Terrorist organizations and extremist groups spread terrorist material (e.g., beheading videos, live streaming terror attacks), recruitment propaganda (e.g., via recruitment magazines), and radicalization campaigns (e.g., stirring up hatred via direct messaging) (Gillespie, 2018, p. 37; Radsch, forthcoming, pp. 3–4). According to Gillespie, "(t)hey do so not just to send specific messages to governments that oppose them and strike fear in those who watch, but also to assert themselves as a powerful group in the public eye, to inspire people to join their cause, to goad other extremist groups to do the same, and to affirm a society in which such acts are possible." (Gillespie, 2018, p. 55) States try to tackle

content that threatens national security. For instance, according to the UK 2006 Terrorism Act, platforms should comply with take-down requests of terrorist content within two days or they are considered as having endorsed this content. In Egypt, Jordan, Qatar, and Saudi Arabia, laws exist that give authorities to surveil online communication suspected to have terrorist activity (Gillespie, 2018, p. 37).

II.2. Regime type

In order to explain variation in control of political and security content, I look at the effect of regime type. In the literature on political regimes, a regime is a "specific set of formal and/or informal rules for choosing leaders and policies." (Geddes et al., 2014, p. 314) Hence, a regime "determines who has access to political power, and how those, who are in power, deal with those who are not." (Fishman, 1990, p. 428) Democracies and autocracies are about political rule, understood as who holds power; the public or a small elite (Debre, 2018, p. 37).

Classifying regime types is increasingly complex since most regimes in the world hold *de jure* multiparty elections, but do not implement *de facto* democratic institutions and processes (Lührmann et al., 2018, p. 1). In his theory of polyarchy, Dahl distinguishes between several institutional guarantees that constitute a democracy, namely elected officials, free and fair elections, freedom of expression, alternative sources of information, associational autonomy, and inclusive citizenship (Dahl, 1971, p. 8, 1998, p. 85). Hence, he does not only assess whether regimes have free and fair elections, but also whether they have certain liberal values and freedoms that would make them meaningful (Lührmann et al., 2018, p. 3).

In order to achieve stability, political systems have to deal with and adapt to demand and challenges from their environment. Therefore, regimes have to counter internal and external threats and challengers (Easton, 1965), which affects human rights practices, such as internet freedoms. In a democratic context, these challengers are actors who want to reverse democratic governance such as disenfranchised autocratic elites. In an authoritarian context, challengers of the status quo can be both democratic (population, international actors) and authoritarian (intra-elites) (Debre, 2018, pp. 193–194). Specific types of internet content can constitute a threat to specific types of political regimes and therefore, these regimes have to control this content. In other words, political regimes (whether democratic or authoritarian) have an interest in controlling internet content, albeit in different ways. I therefore argue that the effect of regime type on content control is conditional on the type of content targeted.

I base my theoretical framework on the literature on domestic conflict. This literature argues that governments use repression when political-economic factors compel coercive behavior, few or no factors hinder repression, and authorities have the capacity to engage with such action (Davenport & Armstrong, 2004, p. 539). Similarly, Davenport argues that political leaders use repression or coercion when there are no mechanisms to counter the coercive power of authorities, there are no consequences for such actions, and there are no alternative mechanisms of control (2007b, p. 10). Hence, there is friction between the possibilities of and constraints on control.

In line with this literature, I argue that the causal mechanism of the relationship between regime type and content control is based on three dimensions: demand, constraints, and alternatives. Demand refers to the political and economic factors that compel control behavior. Constraints refer to the political and institutional factors that constrain or hinder content control. Alternatives refer to the means and tools that states can employ besides requesting intermediaries to remove content for them. For both types of content – political and security – I set out these causal mechanisms and formulate expectations. With regard to political content, I argue that demand for control is higher for authoritarian states than for democracies, that they have fewer constraints and more alternatives. With regard to security content, I argue that demand for control is lower for authoritarian states, that they do not have more or fewer constraints, but that they do have more alternatives. As a consequence, democracies are less likely to control political content but more likely to control security content than authoritarian regimes. For an overview of these causal mechanisms and the expected outcomes, see Table 6.

II.3. Political content

First, with regard to demand for political content control, free flow of information is desired in democracies (Merkel, 2004; Weidmann & Rød, 2019, p. 13). They have a commitment to online freedom of expression, enshrined in national, supranational, and international legal instruments (Breindl & Kuellmer, 2013, p. 372; Ververis et al., 2020, p. 18; J. Wright & Breindl, 2013). Due to their open nature, international pressure and human rights norms also have a larger impact on democracies. Democratic regimes are more embedded in the liberal order than authoritarian regimes, built by the United States and its partners around norms such as economic openness, security cooperation, and democratic solidarity (Ikenberry, 2018, pp. 7, 11). Their embeddedness increases compliance with liberal values and norms, and they become more susceptible to international pressure for protecting political content (Bak et al., 2018, p. 647).

However, the more authoritarian a state is, the less political content is protected. Similar to content on traditional media, online political content is seen as a threat in authoritarian regimes (Weidmann & Rød, 2019, p. 23). When citizens are granted more political rights, authoritarian regimes risk popular mobilization. Popular uprisings occupy a major concern in most autocracies (Svolik, 2012, p. 5) and can be dealt with via coercion through repression (Schlumberger, 2010). Hence, most forms of political organization and public opinion are repressed to prevent collective action. When states can monitor and control political organizations online, these actors become more manageable and political mobilization can be prevented (Weidmann & Rød, 2019, pp. 128–133). Therefore, repression does not have to be exerted through violent means, but also via soft means, such as a restriction of rights or the creation of fear (Davenport, 2007a; Escribà-Folch, 2013).

Second, with regard to constraints to political content, repressive behavior is more costly for democracies than for autocracies (Davenport, 2007a, p. 10), since content control is institutionally constrained by party competition and the rule of law (Stier, 2015, p. 1277). If a government is constrained by an effective legislature and opposition parties, citizens have possibilities to limit political content control (Bak et al., 2018, p. 647). If there are democratic channels available through which citizens can express their concerns about human rights violations, such as the control of political content, incumbent governments can fear political punishment for their actions. Hence, executives can feel threatened by electoral punishment if they resort to certain types of content control and therefore can decide not to (Davenport, 2007a, p. 10; Davenport & Armstrong, 2004, p. 540; Stier, 2015, p. 1277). Moreover, content control by one authority can be resisted and retributed by other political actors (Breindl & Kuellmer, 2013; Davenport & Armstrong, 2004, pp. 538, 540; Ververis et al., 2020, p. 18), and rejected and delayed by constitutional courts (A. Busch et al., 2018, p. 22). Regulatory and legal safeguards in democracies provide protection against governmental overreach, improve the transparency of content control and provide opportunities to citizens to influence internet policies (Hintz & Milan, 2018b, p. 3946).

However, when authoritarian states expect that censorship of political content would be effective, then the cost of content control will be so low that it would hardly constrain a government's decision. In authoritarian regimes, there is a lack of political opposition, which allows for the gradual introduction of political content control (Baldino & Goold, 2014; Ververis et al., 2020, p. 19; Yesil et al., 2017). In even more closed authoritarian regimes, where legislative offices are not filled via contested elections at all (Przeworski et al., 2000; Weidmann & Rød, 2019, p. 13) and the executive power has full authority over decision-making

procedures, citizens do not have any means to prevent content control (Bak et al., 2018, p. 647). If states have no written constitutions or constitutional courts, there are fewer rejections and delays of political content control (A. Busch et al., 2018, p. 22). Hence, institutional constraints are minimal to non-existent and there is a great capacity for state repression (Stier, 2015, p. 1277; Ververis et al., 2020, p. 19; Weidmann & Rød, 2019, p. 6).

Third, with regard to alternatives to controlling political content via intermediaries, the options for democratic states are limited. The more authoritarian a regime is, however, the more options for attempting to control internet communication become possible (Morozov, 2011; Tucker et al., 2017). These alternative methods include using online propaganda (Weidmann & Rød, 2019, p. 31), blocking systems, internet slowdowns, internet shutdowns, algorithmic manipulation of search results (Tucker et al., 2017, p. 51), and hiring trolls (Tucker et al., 2017, p. 55). Weidmann and Rød show that a high level of internet control in authoritarian countries keeps dissent low on the long term, which decreases the frequency of political protest (2019, p. 6): "the resource advantage autocratic regimes enjoy over opposition activists makes Internet control highly asymmetrical, with the government at an advantage." (Weidmann & Rød, 2019, p. 31) Besides digital means, authoritarian states also still resort to traditional strategies of autocratic rule, such as the registration of users in internet cafes (Deibert & Rohozinski, 2010, p. 52), restrictions on press freedom, limiting political association, violent repression of emerging protest (Weidmann & Rød, 2019, p. 146), and arresting opposition (Tucker et al., 2017, p. 55). Even though these alternative strategies are limited in democratic regimes, due to their low demand and high institutional constraints, I expect that they are less likely to request for political content to be removed. Therefore, I formulate the first hypothesis:

Hypothesis 1: The more authoritarian a state is, the more likely it is to request for political content removal.

II.4. Security content

First, at first glance, there seem to be no differences between democracies and autocracies in their demand for security content control. If the internet is perceived as a threat to national security, it is an arena that must be governed (Birnhack & Elkin-Koren, 2003, p. 16). All governing authorities control threats to their political and economic system, and to the lives and beliefs of the people in their territorial jurisdiction (Davenport, 2007a, p. 7). States counter threats to existing power structures (A. Busch et al., 2018; Nisbet et al., 2012; Stoycheff et al., 2018, p. 2) and the status quo via repressive action (Davenport, 2007a, p. 7). Even before the existence of the internet, content control was seen as legitimate and necessary, even in

democracies (Breindl & Kuellmer, 2013, p. 374; Mailland, 2000, p. 1184). Furthermore, political elites in all regimes can seize external threats to push for harsher content control (Baldino & Goold, 2014; Tréguer, 2016; Ververis et al., 2020, pp. 19–20; Yesil et al., 2017).

However, some scholars argue that the demand for repression against criminals and dissidents is even higher in democracies because elections encompass greater challenges to state authority via crime, protest, and terror (Bingham, 1982; Chenoweth, 2010; Conrad et al., 2018, pp. 6, 14; LaFree & Tseloni, 2006). Since more political participation leads to more dissent, there are "more interactions between agents of coercion and people who are unlikely to be members of a winning coalition under electoral contestation." (Conrad et al., 2018, p. 14) In authoritarian states, citizens falsify their preferences (Kuran, 1997), which results in less crime, protest, and violent challenges. As a consequence, there is less demand for combatting criminals and dissidents in authoritarian regimes than in democracies (Conrad et al., 2018, pp. 6–7).

Second, with regard to constraints of security content control, some democratic institutional constraints apply to security content control similar to political content control (e.g., judicial oversight). However, electorates are less critical of leaders in the context of security threats. In fact, democratic regimes can be electorally punished if they fail to control certain content (Bak et al., 2018, p. 647). Citizens delegate their individual protection and safety to the executive power (Conrad et al., 2018, p. 6). Filtering of perceived threats to national security targeted at insurgents, extremists, terrorists, and other threats often receives public support (Faris & Villeneuve, 2008, p. 9). Furthermore, people are more likely to accept human rights violations in response to a threat (Conrad et al., 2018, p. 6; Davis, 2007; Davis & Silver, 2004). Voters prefer that the state does not violate their own rights (Conrad et al., 2018, pp. 6–7), but they are not critical of violations directed at other actors such as criminals, terrorists, and extremists (Conrad et al., 2018, p. 6). As a consequence, in democracies, "leaders are more likely to avoid human rights violations writ large, but still tolerate violations against people who the public perceives as threatening." (Conrad et al., 2018, p. 7) However, harsh responses to terrorism might backfire in democracies, since they "undermine the government's legitimacy and can increase support for terrorist groups, facilitate terrorist recruitment, and prolong the lifespan of terrorist groups." (Daxecker & Hess, 2013, p. 563) At the same time, more authoritarian leaders are less dependent on the perceptions of counter-terrorism policies. They are less dependent on public opinion and therefore less normatively and legally constrained in control of security content. According to Daxecker and Hess, "(a)uthoritarian leaders can (,,,) be less concerned with the public's response to repressive counter-terrorism policies or the

electoral consequences of such actions." (2013, p. 565) Therefore, neither democracies nor autocracies are constrained when they aim to control security content.

Third, with regard to alternatives to security content control via intermediaries, similar to the control of political content, democracies have fewer options than authoritarian regimes. Democracies rely heavily on internet intermediaries to control content in times of instability to reinstate public order (MacKinnon, 2013; Meserve, 2018, p. 56; Meserve & Pemstein, 2018; Stoycheff et al., 2018, p. 3). Strategies of security content control in democracies might be more far-reaching than for the control of political content. For instance, after the Charlie Hebdo shootings in 2015, the Intelligence Act changed the legal basis for content control in France, allowing for circumventing criminal procedures, extrajudicial content control, blocking of websites with terror-related content, and computer hacking for information gathering (Ververis et al., 2020, p. 7). Furthermore, the use of communication surveillance is deemed to protect citizens from crime and terrorism, even when their rights have been infringed (Cammaerts & Mansell, 2020, p. 141). However, democracies do not have the vast array of online and offline alternatives of their authoritarian counterparts, such as internet shutdowns, online propaganda, and using trolls. Hence, there is an enduring structural asymmetry (Tucker et al., 2017, p. 55) with regard to the strategies that democratic and authoritarian regimes can employ to control security content. Hence, democratic regimes are often more restricted in their content control options than authoritarian regimes. When controlling security content, many measures are allowed and justified in democracies, but not anything is possible in internet governance. This leads to the second hypothesis:

Hypothesis 2: The more authoritarian a state is, the less likely it is to request for security content removal.

	Political content		Security content	
Demand	Democracy -	Autocracy +	Democracy +	Autocracy -
Constraints	Democracy +	Autocracy -	Democracy +/-	Autocracy +/-
Alternatives	Democracy -	Autocracy +	Democracy -	Autocracy +
Outcome: Content control	Less likely	More likely	More likely	Less likely

Table 6. Overview of causal relationship between regime type and control of political and security content.

III. Methodology: measurement and estimation

III.1. Dependent variable

The dependent variable, content control, is measured by the total number of items requested to be removed by governments to Google (Google, 2019). I derived this data from Google transparency reports, which makes content control comparable across countries and offers a unique insight into online content control and the restriction of speech (Meserve, 2018, p. 56). This data has great added value because (1) content control data is hard to come by, (2) it is comparable between countries, and (3) it has a broad reach. It is an opportunity to measure online content control endeavors by all countries in the world and compare their behavior.

In the Google transparency data, I assessed the number of items requested instead of the number of requests (which can include multiple items), allowing for more comparable analysis. The data includes both requests via court orders and requests by the executive power and the police (including local, regional, and national authorities), and applies to a broad variety of 'products'.[12] Governments request Google to remove content for specific reasons, after which Google staff assigns each request a reason category,[13] which enables the comparison of states'

[12] These products are AdSense, Android Market, blog searches, bloggers, buzz, chrome web store, feedback, Gmail, Google AdWords, Google Apps, Google Books, Google Code, Google Docs, Google Earth, Google Maps, Panoramio, Google Groups, Google Images, Google News, Google Notebook, Google Photos, Google Places, Google Play Apps, Google Product Search, Google Profiles, Google Scholar, Google Sites, Google URL Shortener, Google Video Search, Google Videos, Google Voice, Google+, Google+ Local, iGoogle, Knowledge Graph, orkut, Street View, Textcube, the internet, web search, web search: autocomplete, web search: related results, and YouTube.

[13] Google distinguishes between the following reasons for requesting content removal: defamation, electoral law, government criticism, adult content, hate speech, impersonation, obscenity/nudity, religious offense, bullying/harassment, drug abuse, geographical dispute, national security, privacy and security, suicide

reasons for content control. These reasons are divided into two different dependent variables, namely government criticism reasons in order to measure political content control (27,640 items in total), and national security reasons in order to measure the control of security content (212,511 items in total). Although the original requests are not made available, anecdotal evidence published in Google's transparency report does provide insight into the detailed content of these categories.

Government criticism content is measured by looking at criticism of local and state government agencies, public officials, and political actors, which includes political leaders, politicians, ambassadors, judges, police, public representatives, mayors, members of the monarchy, and government officials. Topics of criticism include accusations of political corruption, abuse of power, conducting house searches without a warrant, improper business actions, raising of their salary, misuse of public money, corrupt hiring practices, unjust enrichment, money laundering, and bribery schemes. Furthermore, it entails the depiction of state symbols in a disparaging way, criticism of national identity and values, criticism of military history and policy, and patriotic holidays. Finally, it includes content on political campaign ads, pictures and texts of critical books, satire of political leaders and politicians, information on political aims of protesters, and sharing reasons for protesting (Google, 2019).

Security content is measured by looking at content that threatens national security, such as the promotion of terrorism, and terrorist propaganda (e.g., videos glorifying Osama Bin Laden and ISIS, discussing jihad). Furthermore, it includes the promotion by a prohibited organization in its criminal activities, extremist content, entries of prohibited books under anti-extremist and terrorist law, content spread by extremist organizations, and fascist content. Finally, it entails threats to public officials, such as police officers, the protection of public order, the prevention of crime, and the protection of general health (Google, 2019).

If there were no items reported in the data, the variable was coded as '0', leading to an inflation of zero observations. The data ranges from June 2009 to July 2019 and is reported biannually. Since Google started to more accurately record the items requested and reasons for requests since 2011 and most control variables are available until 2017, the analysis of this paper is limited to that period.

promotion, violence, business complaints, copyright, fraud, regulated goods and services, trademark, other, and unspecified.

III.2. Independent and control variables

In order to show the differences between regime types, I use a categorical independent variable instead of a continuous one. Lührmann et al. classified regime type into four categories based on combinations of electoral and liberal principles characteristics: liberal democracies, electoral democracies, electoral autocracies, and closed autocracies. A liberal democracy has free and fair elections, but also legislative and judicial oversight over the executive, protects individual liberties, and has a rule of law (Lührmann et al., 2018, p. 2). They are characterized by additional individual and minority rights and limits on the government (Dahl, 1956). An electoral democracy also has free and fair multiparty elections but only sufficient institutional guarantees of democracy (Lührmann et al., 2018, p. 2). In autocracies, rulers are not accountable to citizens, but there are differences to what extent the chief executive is subject to de jure multiparty elections (Schedler, 2013, p. 2). In electoral autocracies, the chief executive is dependent on a de jure elected legislature, but without any democratic standards such as party competition, these institutions are de facto undermined to avoid accountability (Diamond, 2002; Gandhi & Lust-Okar, 2009; Levitsky & Way, 2010; Lührmann et al., 2018, p. 4; Schedler, 2013). In closed autocracies, the chief executive is not dependent on elections, or there are no de facto or de jure competitive elections (Schedler, 2013, p. 2). Using Lührmann et al.'s regime type classification, I distinguish between four categories, ranging from 0 (closed autocracy) to 3 (liberal democracy) (2018) using the ninth version of the V-Dem data (Coppedge et al., 2019). See Appendix 2 for an overview of which country falls into which category of the Lührmann et al.'s categorization.

I added control variables that might affect how many political opportunities there are for controlling content. I control for the number of terrorist incidents since previous studies have found that governments limit free speech online when facing internal unrest (Meserve, 2018; Meserve & Pemstein, 2018; Stier, 2015). I use the global terrorism database from the National Consortium for the Study of Terrorism and Responses to Terrorism (National Consortium for the Study of Terrorism and Responses to Terrorism (START), 2018). This variable was logged due to a skewed distribution. Some authors argue that more control of corruption can lead to higher degrees of media freedom (Stier, 2015, p. 1278). I measured control of corruption by using the Worldwide Governance Indicators, whereby a higher score means less corruption (Kaufmann et al., 2011). I add civil society organization consultation as another control variable since studies have found that states with more non-governmental organizations are more likely to respect human rights (Hafner-Burton, 2005). The civil society

organization consultation variable has a three-point ordinal scale ranging from 0 (no consultation) to 2 (consultation), converted to an interval scale by the measurement model of V-Dem (Coppedge et al., 2019). Although controlling for all alternatives of content control is methodologically unfeasible, I do take content control alternatives somewhat into account by adding a control variable on government filtering capacity. This variable has a four-point ordinal scale ranging from 0 (lack of any capacity) to 3 (has the capacity), converted to an interval scale by the measurement model of V-Dem (Coppedge et al., 2019). Furthermore, I argue that knowing about illegal content is a precondition for controlling that content. Therefore, I control for government social media monitoring, which is a five-point ordinal scale ranging from 0 (extremely comprehensive) to 4 (not at all), converted to an interval scale by the measurement model of V-Dem (Coppedge et al., 2019).

Other control variables are more structural and economic. Higher internet penetration has deterrence effects on control since it facilitates negative publicity of repression (Bak et al., 2018). I measure internet penetration rates by the percentage of internet users per country via the World Development Indicators (ITU, 2019). I control for economic development because economies with scarcity are more likely to repress threats (Poe et al., 1999). I measured GDP per capita in constant 2010 US dollars via the World Bank and OECD national accounts data (World Bank & OECD, 2019). This variable was logged due to a skewed distribution. Studies have found that foreign direct investments reduced the coerciveness of political leaders (Hafner-Burton, 2005) and improved human rights (Blanton & Blanton, 2007; Richards et al., 2001), and might therefore also reduce their content control. Foreign direct investment net inflows were measured as a percentage of GDP using the World Development Indicators (ITU, 2019). Finally, population size is a predictor of content control, since larger populations increase opportunities for rebellion and, as a consequence, repression (Henderson, 1993; Poe et al., 1999). I measured population size via the UN Population Division and other organizations (United Nations Population Division et al., 2019) and logged due to a skewed distribution. Only countries with a population of 500,000 or higher were included in the dataset. See Appendix 3 for an overview of the descriptive statistics.

III.3. Model estimation

For zero-inflated data,[14] one can estimate either a zero-inflated model or a hurdle model in RStudio (version 1.0.153). With zero-inflated data, I mean data that contains a high frequency

[14] I.e., data that contains a high frequency of zero observations. In the context of this paper, that means there is an excess of governments that do not request for any content to be removed.

of zero observations. In the context of this paper, it means an excess of governments that do not request for any content to be removed. Since there is only one 'source' of zeros, namely that a government did not request removal even though they had the opportunity to do so (Hofstetter et al., 2016, p. 521), a negative binomial hurdle model was estimated. A hurdle model consists of two parts. First, there is a zero hurdle part which is a binary logistic regression assessing the odds of requesting content removal. Second, there is a count part assessing the effects for those governments that engage in content removal requests (i.e., the counts that exceed zero). For the count part, a negative binomial distribution was selected, since there is overdispersion (Hofstetter et al., 2016, p. 522). In order to account for the multilevel structure of the data (i.e., the number of items requested by governments over years), I added year fixed effects to assess the effects between countries over years. Since regime type is a relatively stable variable over time, it is not possible to look at variation within countries across a time span of seven years. See Appendix 4 for R script of the data management and Appendix 5 for the R script of the analysis in R code.

IV. Analysis

IV.1. Trends and differences between states

In Figure 3, I show a number of country-specific trends of items requested to be removed issued to Google from January 2011 until July 2019. There seems to be a rising trend in removal requests, which is similar in both democratic countries (e.g., France, United Kingdom, United States) and authoritarian regimes (e.g., China, Russia). A decomposition of this trend of all countries in the world (see Appendix 6) shows that there was no clear trend in the items requested to be removed until 2015, after which there is a slight decline and a steep upward trend since 2016. Globally, states increasingly request intermediaries to remove items from their platforms since 2016.

In Figure 3, the number of requests varies widely per country and there is no clear distinction between democratic and authoritarian regimes. Although Russia requested almost 182,462 items to be removed between January and June 2018, the United States also requested for 39,902 items to be removed between January and June 2019, and both countries show a steep upward trend. China requests only a limited number of items to be removed, although we also see an upward trend here since December 2017 (regardless of the Great Firewall of China which already blocks most foreign content). Similar numbers, however, can be seen in Germany. So far, by eyeballing the data, it seems that – just as authoritarian regimes – democratic states request content removal to intermediaries and all regime types actively

attempt to control internet content. The proportion of national security reasons in the total number of items requested does seem to be larger for democracies than for autocracies. Therefore, I will assess more systematically how regime type is related to content control.

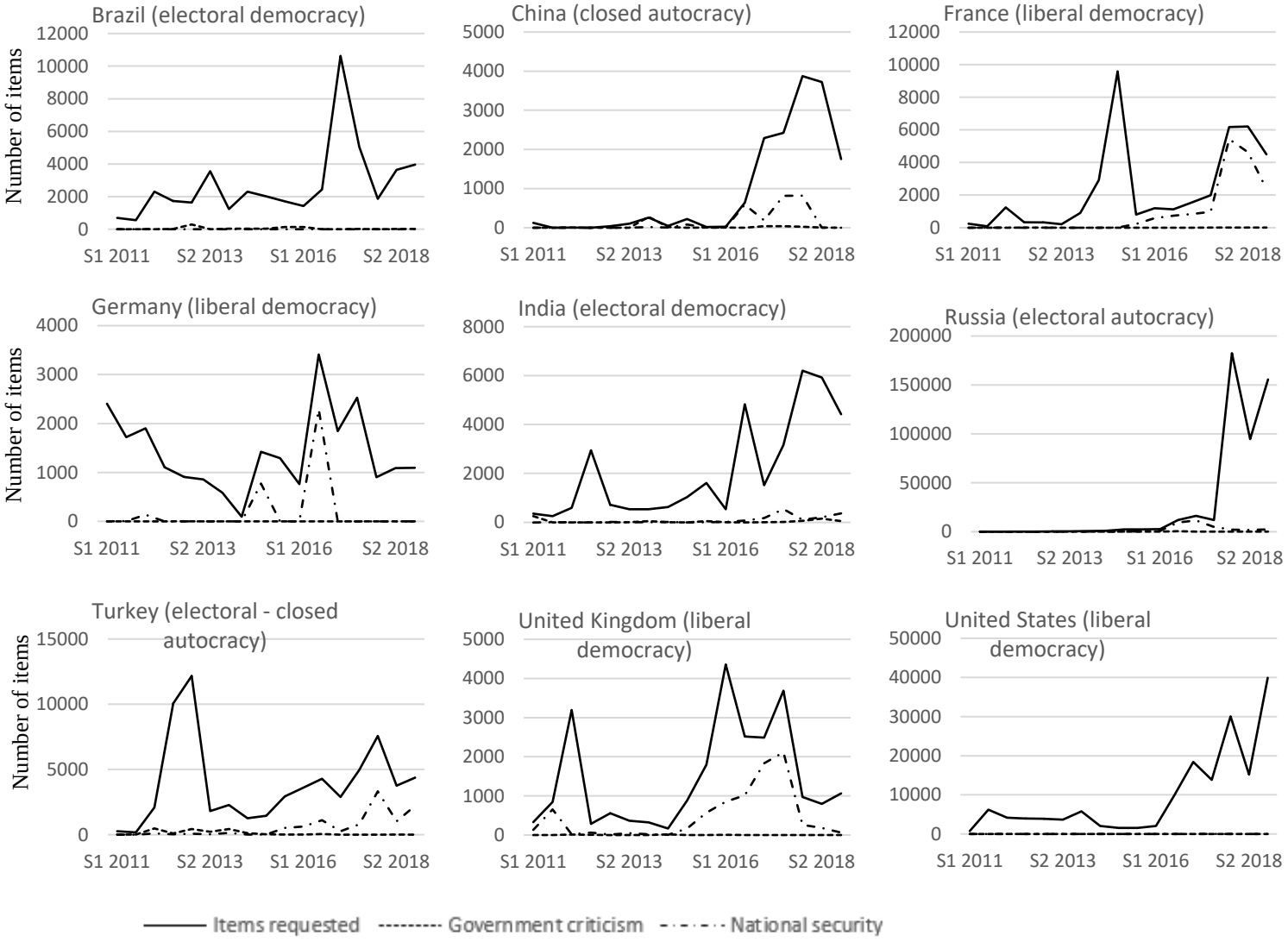


Figure 3. Country trends of items requested to be removed to Google, January 2011-July 2019.

Note: the scales on the y-axes differ between countries to maximize the readability of the figures.

IV.2. Government criticism content model

When assessing the relationship between regime type and requests for removal of political content in the zero part in Model 1 of Table 7, I show that electoral democracies and electoral autocracies are less likely to turn to request the removal of government criticism content than liberal democracies. Coefficients are reported in log odds. There are differences

between regimes, but this does not per se mean that these differences can be attributed to regime types themselves. In order to test whether these differences can be explained by regime types themselves or possible cofounders, I include the control variables in Model 2. In Model 2, there is some indication ($p < 0.1$) that electoral democracies are more likely to turn to request government criticism to be removed than liberal democracies. The odds ratio of requesting government criticism content removal is $\exp(0.96) = 2.61$. This means that electoral democracies are 2.61 times more likely to turn to removal requests than liberal democracies. For the control variables, I find that higher economic growth is related to turning to government criticism content removal requests. Furthermore, countries with a larger population are more likely to turn to request for political content to be removed. I also find a statistically significant positive effect for terrorist incidents (albeit at $p < 0.1$ level). Hence, liberal democracies are more likely to turn to request the removal of political content in the zero hurdle model, but this can mainly be attributed to other variables, such as economic growth and population size.

When assessing the count part of the model, I zoom in on those states that are already engaged in requesting government criticism content to be removed. In Model 3, there is a significant positive effect of electoral democracy, electoral autocracy, and closed autocracy relative to liberal democracy. For this part of the model, these are still the differences between regime types without controlling for other variables. When we add control variables in Model 4, the results show again significant differences between liberal democracies and the other regime types. For instance, the statistically significant rate ratio for electoral autocracies is $\exp(3.27) = 26.31$ in Model 4. In other words, once a government is involved in requesting the removal of government criticism content, it requests 26.31 times more content to be removed if it is an electoral autocracy relative to a liberal democracy. Similarly, closed autocracies request $\exp(5.02) = 151.41$ times more government criticism content removals than liberal democracies. The size of the effects remains robust when controlling for other variables. With regard to the control variables, none are statistically significant. Hence, the more authoritarian a state is, the more likely it is to request the removal of government criticism content.

The closed autocracies that ask for the removal of political content are China, Kuwait, Saudi Arabia, Thailand, the United Arab Emirates, and Vietnam. The electoral autocracies that turn to political content removal requests are from different parts of Asia (i.e., Armenia,

Bangladesh, Iraq, Kazakhstan, Malaysia, Pakistan,[15] Russia, Thailand,[16] Turkey,[17] and Yemen), and Kosovo and Ukraine. The electoral democracies that request the removal of government criticism content are mainly Latin American (i.e., Argentina, Brazil, Colombia, Jamaica, Mexico, Peru), South East Asian (i.e., Indonesia, Philippines, Thailand), or South Central Asian (i.e., India, Pakistan). Furthermore, Hungary and Turkey belong to this group. If we assess the liberal democracies requesting government criticism to be removed, some of them are European states (i.e., Austria, Denmark, France, Germany, Poland, Spain, United Kingdom). Australia, Canada, and the United States also request the removal of government criticism content, just as Israel, Japan, Mauritius, South Korea, and Trinidad and Tobago. See Appendix 2 for an overview of which countries and regime types turn to removal requests for different types of content.

To summarize, in the zero part of the model, electoral democracies and electoral autocracies were less likely to turn to government criticism content removal requests than liberal democracies. However, this effect was accounted for by cofounders, such as economic growth and population size. When I zoom in on those states that already engage with government criticism content removal requests in the count part of the model, there is a robust positive effect for all categories. The effects of regime type are large, statistically significant and the regime type variables are the only statistically significant predictors in the full model, indicating the explanatory factor of regime type in the control of political content. Hence, albeit true that democracies control internet content, there is a statistically significant difference between democracies and autocracies. The further one goes down Lührmann et al.'s scale in the direction of closed authoritarianism (2018), the more likely states attempt to control online political content. Therefore, I find strong support for the first hypothesis.[18]

[15] Pakistan transition from and electoral democracy to an electoral autocracy in 2013.
[16] Thailand transitioned from an electoral autocracy to an electoral democracy in 2012, to an electoral autocracy in 2013, and to a closed autocracy in 2014.
[17] Turkey transitioned from an electoral democracy to an electoral autocracy in 2013.
[18] The more authoritarian a state is, the more likely it is to request for political content removal.

	Dependent variable: government criticism content control				*Dependent variable*: national security content control			
	Zero hurdle model		Positive count model		Zero hurdle model		Positive count model	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Electoral democracy	-0.59*	0.96$^{\#}$	2.89***	2.28*	-1.12***	1.11$^{\#}$	-1.27**	-1.32
(ref = liberal democracy)	(0.27)	(0.58)	(0.40)	(0.95)	(0.27)	(0.62)	(0.47)	(1.42)
Electoral autocracy	-1.10***	0.65	3.98***	3.27**	-0.96***	1.68*	1.79***	-1.25
(ref = liberal democracy)	(0.30)	(0.76)	(0.45)	(1.15)	(0.25)	(0.79)	(0.44)	(1.90)
Closed autocracy	0.23	1.11	5.59***	5.02***	-0.39	0.16	-0.87	-3.49$^{\#}$
(ref = liberal democracy)	(0.33)	(0.80)	(0.48)	(1.22)	(0.35)	(0.82)	(0.59)	(1.81)
Control of corruption		-0.02		-0.43		-0.01		-0.76
		(0.30)		(0.57)		(0.30)		(0.76)
Internet penetration		0.01		0.00		0.04**		0.05$^{\#}$
		(0.01)		(0.02)		(0.01)		(0.03)
Log economic growth		0.95***		0.11		0.72*		-0.09
		(0.28)		(0.51)		(0.30)		(0.52)
Log terrorist incidents		0.07$^{\#}$		0.08		0.03		-0.05
		(0.04)		(0.07)		(0.04)		(0.07)
Civil society organization		0.03		0.19		0.37$^{\#}$		0.54
consultation		(0.19)		(0.32)		(0.19)		(0.35)
Filtering capacity		-0.08		0.10		0.34$^{\#}$		1.33**
		(0.20)		(0.44)		(0.21)		(0.39)
Social media monitoring		-0.23		-0.09		-0.43*		-1.04**
		(0.16)		(0.25)		(0.18)		(0.34)
Foreign direct investment		-0.06		-0.05		0.01		0.00
		(0.04)		(0.09)		(0.02)		(0.04)
Log population size		0.96***		0.05		1.15***		0.31

		(0.13)		(0.22)		(0.13)		(0.26)
Constant	-1.65***	-28.20***	1.24***	-0.61	-1.33***	-32.27***	5.11***	-4.03
	(0.22)	(3.40)	(0.27)	(6.05)	(0.25)	(3.67)	(0.27)	(7.08)
Log Likelihood	-302.99	-199.33			-330.71	-195.79		
Observations	890	890	101	101	890	890	117	117
Nagelkerke R^2			0.61	0.63			0.60	0.70

Coefficients in log odds, std. error in parentheses,
$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$, $^{\#}p < 0.1$.

Table 7. National security and government criticism content removal requests hurdle model.

IV.3. National security content model

As shown in Table 7, the effects for the zero part look quite similar to the government criticism model. Again, in Model 5, the negative effects are statistically significant for both electoral democracy and electoral autocracy compared to liberal democracies. When controlling for other variables in Model 6, the effects for electoral democracy and electoral autocracy become positive. For instance, in the zero part in Model 6, the odds ratio of turning to request removal of security content for electoral autocracies is exp(1.68) = 5.37. Hence, electoral autocracies are 5.37 times more likely to turn to content removal requests than liberal democracies. Again, there is no statistically significant effect for closed autocracies in the zero part of the model (both Model 5 and 6). For the control variables, I find that states with higher internet penetration rates, economic growth, and population sizes are more likely to turn to security content control. Moreover, Model 6 shows some indication ($p < 0.1$) for a positive effect of civil society organization consultation and filtering capacity. Interestingly, states that engage in more social media monitoring are less likely to turn to request the removal of national security content. Hence, the negative effects of the regime types in Model 5 cannot be attributed to the differences between regime types themselves, but are suppressed by the control variables. Liberal democracies are more likely to turn to request the removal of national security content based on Model 5; not because they are democracies, but because they have larger internet penetration rates, economic growth, filtering capacities, degree of social media monitoring, and population size. When I control for these and other factors, the model even indicates electoral democracies and electoral autocracies are more likely to turn to national security removal requests compared to liberal democracies.

The count model (Model 7 & 8) assesses the effects for the number of national security items requested to be removed, for those governments that are already engaged in content removal. In Model 7, electoral democracy has a statistically significant negative rate ratio and electoral autocracy has a positive rate ratio compared to liberal democracies. Hence, electoral democracies request more national security content removal than liberal democracies and electoral autocracies request less. These are the differences between regime types, without taking into account correlation with other explanations. When controlling for additional variables in Model 8, these differences are no longer statistically significant. In Model 8, the rate ratio for closed autocracy is exp(3.49) = 0.03. Hence, within the group of countries that engaged in the removal of security content, closed autocracies are 0.03 times less likely to request national security content removal than liberal democracies. However, the difference

between liberal democracies and closed autocracies has a low significance level ($p < 0.1$) and there is no statistically significant effect for electoral democracies and electoral autocracies. Hence, there is only a weak indication that there are differences between regime types.

The closed autocracies that engage in the removal of security-related content are China, Hong Kong, Saudi Arabia, Thailand, United Arab Emirates, and Vietnam, and therefore quite similar to the ones requesting government criticism content to be removed. If we assess which liberal democracies engage in the removal of security content, there are more European states relative to those liberal democracies that requested government criticism to be removed (i.e., Belgium, France, Germany, Italy, Netherlands, Poland, Spain, Switzerland, United Kingdom) or Western (i.e., Australia, Canada, United States), with the exception of Israel, Japan, and South Korea.

With regard to control variables, filtering capacity has a statistically significant positive effect in both zero and count models (Model 6 and 8), indicating that when states control information via blocking access to certain websites, they are also more likely to turn to content removal requests. Once they engage in content removal, they also are going to submit, more national security content removal requests. Similarly, with regard to social media monitoring, there is a statistically significant negative effect in both models (the highest score on this variable means 'no monitoring'). This indicates that when states surveil more content on social media, they request more removal of national security content. A higher degree of monitoring means more surveillance of internet content and as a consequence, leads to an increase in control of that content. Furthermore, the higher internet penetration rates are, the more national security content removal governments request, possibly because the internet is then expected to have a wider reach and impact on society.

To summarize, in the zero part of the model electoral democracies and autocracies are less likely to turn to national security content removal requests than liberal democracies. However, this effect can be mainly attributed to larger internet penetration rates, economic growth, more social media monitoring, and population size. Hence, liberal democracies are more likely to turn to control of security-related content, because of these characteristics. Furthermore, once these liberal democracies are engaged in content removal, they request more removal of security content than closed autocracies, but there are no significant differences between electoral democracies and autocracies on the one hand and liberal democracies on the other Altogether, there is some support for the second hypothesis,[19] but there is also an

[19] The more authoritarian a country is, the less likely it is to request for security content removal.

indication that liberal democracies, electoral democracies, and electoral autocracies do not differ much when it comes to controlling security-related content.

V. Conclusion

This paper aimed to analyze content control by governments and the reasons for these requests by using removal request data from Google transparency reports. In this broad empirical study that compares content control between all countries in the world – democracies and autocracies –, I show that content control is on the rise. However, I also show that there are significant differences between different types of content. Liberal democracies are less likely to control political content than electoral democracies, electoral autocracies, and closed autocracies. I found some evidence that they are more likely to request the removal of security-related content. There is also an indication that liberal democracies, electoral democracies, and electoral autocracies do not differ much with regard to security content control. Furthermore, I found an indication that this relationship can partly be explained by higher internet penetration rates, economic growth, filtering capacity, social media monitoring, and population size in democracies. Hence, democracies do control internet content, but the effect of regime type is conditional on the type of content targeted. These results have three implications for internet governance research on content control.

First, the often-underlying assumption that democracies do not control content (see, for instance, Dick et al., 2012; OpenNet Initiative, 2012) is not accurate. Although some parts of the internet governance literature have started to acknowledge that democracies can control content (see, for instance, A. Busch et al., 2018; Deibert et al., 2010; Hintz & Milan, 2018b; Meserve & Pemstein, 2018; Yangyue, 2014), I argue that the type of content targeted matters for the relationship between regime type and content removal requests. Especially the degree of security content control is remarkable and implies that a broad conceptualization of security content poses a risk to democracies. Based on the findings that democracies are more active than closed autocracies in controlling security content via intermediaries, and that this control is seen as legitimate in democracies, framing content in such a manner would enable its censorship. Internet governance debates are predominantly defined by a security narrative (Hintz & Milan, 2018b, p. 3949) and news media coverage often justifies and normalizes surveillance and disregards civil liberties (Wahl-Jorgensen et al., 2017). Hence, security concerns about content can only be justified if that content is actually about security issues. However, if it is not, security concerns become a fig leave for broader content control. Some

scholars even argue that democracies are converging with more authoritarian regimes by normalizing internet and content regulation (A. Busch et al., 2018; J. Wright & Breindl, 2013). When security threats occur and states of emergency are invoked, they legitimize sudden and sharp increases in control (Ververis et al., 2020, p. 7). Furthermore, there is a risk that once any form of content control occurs, elites are tempted to expand it (Warf, 2011), accelerating "a race to the bottom." (Stoycheff et al., 2018, p. 3)

Second, differentiating between types of content is meaningful. Since the effect of regime type on political and security content control has different directions, this also raises the question of what the relationship is between regime type and other types of content. Examples of such content (which could be categorized in several ways) include sexually explicit content, hate speech, self-harm, misogynistic content, racist content, homophobic content, trolling, harassment (Gillespie, 2018, pp. 36–37), gambling, and intellectual property rights (P. Pearce et al., 2017; Ververis et al., 2020, p. 2). For example, I would expect that the demand for controlling content dependent on social, cultural, and religious norms is higher in more authoritarian regimes. However, I would expect states that have a high interest in the information economy (such as the US) to have a higher demand for controlling content such as intellectual property. I would expect some content to be universally contested, such as child abuse material or youth protection in the context of violence (Breindl & Kuellmer, 2013, p. 372; Deibert et al., 2012).

The findings of this research tie in with the debate in the political regime literature on the differentiated impact of regime type on repression. It shows that democratic political institutions can only limit certain types of control and that the importance of distinguishing between types of coercive behavior (Davenport, 2007b, pp. 11–12). It is in line with a growing literature that argues that democracies are only able to limit repression in specific contexts, by showing (1) the importance of distinguishing between different types of content and (2) that democratic political institutions only decrease specific forms of repression within certain contexts (see, for instance, Conrad et al. (2018), Von Soest & Grauvogel (2017)).

Third, the strong reliance of democracies on intermediaries raises new interesting questions for democratic principles and oversight of content control. Collaborations between states and private companies are often executed in regulatory twilight zones (Elkin-Koren & Haber, 2016, pp. 107, 115). This governance by proxy can evade the rule of law and bypass institutional constraints since private actors have neither constitutional limits concerning content control nor duties to protect freedom of speech online (Boyle, 1997, p. 202; Breindl &

Kuellmer, 2013, p. 382; Brown, 2010; Ververis et al., 2020, p. 7). Even if content is legal, an intermediary can decide to remove it based on its terms of service (Hintz, 2016, pp. 325–326), creating incentives for governments to request the removal of certain content even if it falls within legal frameworks. Content control via intermediaries implies an 'outsourcing' (McIntyre, 2013) of internet censorship. Hence, this poses challenges to protecting freedom of speech online in liberal democracies.

This study opens up new avenues for future research. More comparative analyses of content control between regime types are necessary, specifically focusing on the causal mechanisms at play, such as the role of government effectiveness and the rule of law. Some control variables, such as the government filtering capacities, social media monitoring, and internet penetration rates also had statistically significant effects in some models and it would be interesting to explore those further. Future research could also look into other dependent variables, such as user data requests to further explore governance via intermediaries, or the compliance rates of intermediaries to government requests to further address the relationship between public and private actors. The data provided by transparency reports is extensive and overcomes the obstacle of a lack of cross-national digital content control data availability and should be explored more extensively. Similarly, other comparative data on content control, such as data from the Open Observatory of Network Interference (OONI, 2019) and Censored Planet (2019) remains largely unexplored by political scientists. The field of content control could greatly benefit from a more structural synthesis between computer science and network engineering data on the one hand, and political science theory and research design on the other. This research made a first step in showing the reasons for content control efforts and that even democracies try to control the internet under certain circumstances.

CHAPTER 5

Conclusion

Daniëlle Flonk

I. Answer to the research question

After having analyzed broader conflicts over norms and institutions, illiberal norm entrepreneurship, and the variation in content control practices, I want to come back to the research question of this dissertation: *How and why do international content control norms emerge and develop?*

Starting at the *how* part of this question, there are two aspects to how this dissertation answers it. First, I showed that conflicts over content control norms and institutional structures are dependent on the identities involved in those conflicts. In Chapter 2, I (together with my co-authors) showed that there are different spheres of authority that clash over internet governance norms and institutions. The authoritarian proponents of the sovereigntist sphere want to have state control over the internet and protect domestic sovereignty via intergovernmental institutions. The democratic adherents of the liberal sphere support a more open, multistakeholder internet governance model based on self-regulation.

In Chapter 3, I showed that authoritarian norm entrepreneurs such as Russia and China push for content control norms in regional and international organizations. As they are proponents of the sovereigntist sphere of authority, they pursue broadly defined information security norms, whereby states are the core actors in cyberspace. These authoritarian states promote content control norms actively, consistently, and over time. This is very much a paradox: the aim of these international norms is to recognize "a mutual right to make information flows respect national boundaries." (Mueller, 2017, p. 82) Hence, it is a type of multilateralism that is hollow, because it functions as a legitimation of national content control practices. Meanwhile, global institutional capabilities to control content and a strong consensus among states about what should be controlled, remain absent (Mueller, 2017, p. 110).

In Chapter 2, I argued that democracies do try to preserve international open internet norms, but at the same time, EU member states and the US have diverging regulatory regimes, leading to conflict and contradictions. For instance, due to the strong reliance on self-regulation, there is only weak legitimate political authority. They also struggle in the context of security content. Therefore, proponents of the liberal sphere might support intergovernmentalism and illiberal norms when they are dealing with core state powers aimed at crime, terrorism, harmful content, and disinformation. As I have argued in Chapters 3 and 4, democracies are susceptible to controlling security content, and this creates opportunities for autocracies if they want to promote content control norms. By securitizing content, Russia and China find common ground among less-likeminded states. Hence, the liberal sphere is not only challenged externally but

also from within. Whereas proponents of the sovereigntist sphere will continue the promotion of illiberal norms, adherents of the liberal sphere are moving towards more regulation and an increased role of the state in content control.

States draw upon different sets of norms: the sovereigntists from non-interference, and the liberals from the area of human rights. Because these states' goals are often divergent, the proponents of the sovereigntist and liberal spheres clash over deeper norms and institutional structures concerning the openness of the internet. In Chapters 2 and 3, I showed several instances whereby the sovereigntists attempt to challenge existing internet governance institutions and norms, such as the Code of Conduct for Information Security and the UNGGE. Sometimes, this even leads to the creation of competitive regimes in the area of internet governance, such as the revised ITRs.

Second, institutional structures create opportunities and constraints to the norm promotion strategies that states use. In Chapter 3, I showed that Russia and China vary their norm promotion strategies across regional and international organizations. In regional organizations such as the CSTO, SCO, and the BRICS, norm entrepreneurs face more like-minded authoritarian states. In this limited homogeneous context, they are more likely to use socialization strategies: they praise norm-conforming behavior, raise the status of target groups, and exchange expertise. In international organizations such as the UN and WIC, they face less like-minded states. In this broader heterogeneous context, they are more likely to use persuasion strategies: they use argumentation to convince others, such as security frames. These strategies become even more effective when Russia and China sequence them: they build strong regional norms, after which they try to expand their range internationally (and sometimes succeed in doing so). Hence, authoritarian norm promotion strategies are dependent on their organizational context and target audience. Although I did not test this in this dissertation, I expect the same to hold for democratic norm entrepreneurs.

Coming to the *why* part of this question, I zoomed in on the content control practices of different regimes. In Chapter 4, I showed that not only authoritarian states control content, but democracies do so as well. However, they do so for different reasons. Autocrats are more likely to control political content criticizing the government. Demand by states for controlling political content is higher in autocracies than in democracies since content is seen as a threat to incumbents, for instance, because they fear popular uprisings (Schlumberger, 2010; Svolik, 2012, p. 5). Autocracies also have fewer constraints since there is a lack of party competition and rule of law that would allow for government criticism. Autocracies do have more

alternatives to requesting intermediaries to remove content for them, for instance, online propaganda, internet shutdowns, or internet slowdowns.

The often-heard assumption that democracies do not control content is inaccurate (see, for instance, Dick et al., 2012, p. 7; OpenNet Initiative, 2012). Democracies also control content but mainly security-related content, such as terrorist and extremist content. The demand for controlling such content is actually higher in liberal democracies than in closed autocracies, because popular demand for combatting crime and dissidents is higher in democracies since they encompass greater challenges to state authority. Moreover, democracies are not more constrained than autocracies when controlling security content, and electorates are less critical of leaders when there is a security threat. Finally, democracies rely heavily on intermediaries to control content in times of instability and to reinstate the public order.

Hence, content control practices are dependent on the type of content targeted. Democratic political institutions can only decrease specific forms of content control within certain contexts and might even boost content control in other contexts. Due to these differences in demand, constraints, and alternatives, we see a variation in content control practices between regimes. And those practices translate to the international level, where they promote content control norms accordingly.

II. Theoretical and empirical implications

The findings of this dissertation have both theoretical and empirical implications for content control research and internet governance research more broadly. Theoretically, this dissertation shows that an analytic eclectic application of international relations theory contributes to the understanding of content control norm emergence and development. By extension, utilizing theoretical aspects of social constructivism, liberalism, and neoliberal institutionalism could increase our understanding of broader developments in internet governance.

Academics have only recently started to use international relations concepts to analyze internet governance. This dissertation contributes to this debate by showing the applicability of comparative politics and international relations theory to the field of internet governance, while still providing a unique causal framework. My eclectic theory of content control allows us to better understand the internet governance field. First, states subscribe to content control norms, which range from liberal to illiberal norms. Since content control is also about the justification of those practices, states cooperate and promote international content control norms. Second, the behavior of content control actors is dependent on their identities. Regime type has an effect

on which content is being controlled. It also affects how these policies are justified and which norms are being pushed for. Hence, the norms and decision-making procedures promoted in international institutions are a mirror image of domestic democratic and authoritarian values and decision-making procedures. Third, the behavior of actors is dependent on their placement within the global system. It matters to which sphere of authority states belong. Furthermore, whether they operate in a regional or international organization changes the strategies they use for norm promotion.

The literature on internet governance is still not tied to the international relations literature systemically and core global governance concepts are often underused. I come to an eclectic theory of content control by combining theoretical elements from the literature on constructivism, political regimes and liberalism, and neoliberal institutionalism. This dissertation contributes to internet governance research by providing an integrated theoretical framework that uses core international relations concepts such as international norms, political regimes, and international institutions. It shows that the internet is a policy field like any other and that international relations literature allows us to better understand the developments in internet governance more broadly, but also in a specific sub-field such as content control. Scholars should continue this more rigorous embedding of international relations into internet governance.

For instance, earlier accounts in the norm literature subscribed to norm development as a mostly linear process (Finnemore & Sikkink, 1998; Risse-Kappen et al., 1999), whereby the emergence of a norm leads to its cascade and ends in broad support. However, more recent norm research acknowledges that norm promotion and development is a far more contested process (Jose, 2017; Stimmer & Wisken, 2019; Wiener, 2014; Wunderlich, 2014), whereby norm contestation is "the range of social practices, which discursively express disapproval of norms" (Wiener, 2014, p. 1). Hence, norm development is not a linear process, but a process filled with conflict, ambiguity, and different interpretations of how actors should behave according to a norm (Jose, 2017, p. 3). My norm research contributes new insights to internet governance debates, for instance by showing that norm entrepreneurs adapt their internet governance norm promotion strategies to different regional and international contexts. Norm entrepreneurs proactively combine these strategies to more actively promote and develop content control norms. And when positions and identities diverge, norm entrepreneurs clash with other actors over these new norms.

Empirically, there are three broader implications of my findings for the field of internet governance. First, whereas the internet used to be transnationally oriented, I show a move towards nationalization and regionalization. As Mueller stated, "all networks on the Internet are globally connected but locally configured." (2017, p. 49) It seems that this local configuration is increasingly in line with either national or regional borders. Nationally, there are increased content control practices, which can be liberal but also illiberal. And they occur in democracies and autocracies. This is an indication that states try to regain their control over their borders and territory (Goldsmith & Wu 2008). Regionally, I showed an increased exchange of expertise on content control norms and practices. Whereas other norms such as data governance might conflict between regions or states, content control norms can often be stacked. A myriad of global, regional, national, and subnational content control policies do not necessarily clash. The result, however, is a further limitation of freedom of speech online, without users sometimes even noticing that their content is being altered or removed.

Second, instead of upholding an open and unregulated internet, internet regulation is increasing. Whereas the internet was never without regulation (Lessig, 2000; McIntyre, 2013), I showed increased legalization of the internet. Democratic and authoritarian states, regional organizations, and international organizations all increasingly aim to regulate the internet. This dissertation looked at a subset of that regulation, namely content regulation. Whereas in earlier debates, content regulation was seen as an autocratic practice, even democracies now increasingly argue that it is necessary to control certain types of content. In the EU, there is an increased demand for controlling harmful content, which is not necessarily illegal (EC, 2018a, 2018b, 2019). Even in the US, there is more demand for such regulation after indications of election meddling by foreign actors (Farrell & Newman, 2021). This trend will most likely continue in the future.

Third, I observed an increased securitization of content allowing for a limitation of freedom of speech online and increased content regulation. For a long time, scholars assumed that the internet would improve human rights as a liberation technology (Diamond, 2010). However, I showed an increased limitation of freedom of speech online. This dissertation pointed in the direction of the securitization of content as a relevant explanation. I showed in Chapter 4 that the degree of security content control in democracies is remarkable, which implies that a broad conceptualization of security content poses a risk to liberal democracies. In Chapter 3, I argued that authoritarian states and coalitions exploit security frames to push for international content control norms. Hence, securitization is important for finding common

ground in content control norm promotion. The effect is, however, an increased limitation of freedom of speech online.

The assumption presented in the introduction that the internet is an open space that is difficult to regulate does not hold when we look at these broader developments. Existing global internet governance models are contested and countermodels are emerging. Therefore, some scholars signal a move towards a splinternet that is highly balkanized or fragmentized (Drake et al., 2016; Mueller, 2017). Other scholars argue that it is a contestation of the information order itself (Farrell & Newman, 2021). I showed that even with the creation of competitive regimes, it is still too early to call whether internet governance is fragmenting permanently. However, when we take the three points above together, this dissertation goes beyond the discussion of the return of the state in internet governance or a fragmentation of the internet. It shows that a return of the state is not only about an increased role of the state vis-à-vis other actors. States utilize regional organizations to exchange expertise, build consensus and deepen norms. There is an increasing amount of content regulation on national, regional, and international levels. And states use international content control norms to justify content control practices, which range from liberal to illiberal.

III. Future research

The internet order that was considered open and liberal is increasingly contested by both liberal and illiberal actors. A free flow of information across borders is limited and states take a more central role in internet governance. Future research should look into the contestation of what was once considered the open internet order. I make three suggestions on this front.

First, one could look more closely at the explanations and consequences of the internal contestation of the open internet order by liberal actors. This dissertation has shown an internal contestation of the open internet order in three ways. Chapter 2 demonstrated a liberal sphere of authority that is gradually shifting towards more regulation. In Chapter 3, I showed how authoritarian states exploit the security logic of content control to push for illiberal internet norms. In Chapter 4, I showed how, under specific circumstances, democracies also control content. I showed that there are no clear differences between liberal democracies (e.g., European countries, Australia, Japan, South Korea, US), electoral democracies (e.g., Argentina, Brazil, Colombia, Indonesia, India), and electoral autocracies (e.g., Azerbaijan, Belarus, Kazakhstan, Russia, Singapore) when it comes down to controlling security content. This might imply that the distinction between electoral democracies and autocracies is diminishing,

especially in the area of security content control. Accordingly, some scholars have signaled that democracies are converging with autocracies by normalizing internet and content regulation (A. Busch et al., 2018; J. Wright & Breindl, 2013). In the past, we have seen that many closed autocracies shifted into the electoral autocracy category by organizing fake elections and election monitoring (Gandhi & Lust-Okar, 2009; Knutsen et al., 2017). This dissertation shows that liberal and electoral democracies are shifting towards the electoral autocracy category due to their content control values and capabilities. Hence, it is paramount to further explore the contestation of the open internet order by liberal actors. For instance, to what extent does this actually constitute a contestation of the open internet order itself, or is it just a shift of the liberal sphere of authority? To what extent is a 'third way' in internet governance on the rise, as an alternative to the 'Chinese' and 'Californian' models? What is the effect of alternative internet governance models and increased regulation on content control norms?

In other words, more research is needed on the drivers, processes, and effects of the internal contestation of the open internet order. This dissertation has pointed towards a number of explanations. In Chapter 2, I argued that the liberal sphere of authority suffers from internal inconsistencies because it enshrines a weakness of political authority and a demand for domestic stability and security. In Chapter 3, I showed that the securitization of content can provide common ground for developing new norms between democracies and autocracies. This dissertation also argued that content control is a global norm in emergence. It is not only autocracies that control content, but actors within the liberal sphere of authority increasingly lean towards more regulation of harmful and terrorist content (Kierkegaard, 2007). Hence, the role of the state in controlling internet content is increasing. To what extent the emergence of content control norms constitutes a fragmentation of global internet governance is a topic for future debates.

Second, scholars should assess what contributes to successful contestation by illiberal actors. This dissertation has shown an external contestation of the open internet order by autocrats. In Chapter 4, I showed some illiberal content control practices by authoritarian states. In Chapter 3, I showed attempts by illiberal actors to promote illiberal norms. Similarly, in Chapter 2, I showed the attempts by proponents of the sovereigntist sphere to create competitive and parallel regimes. There have been recent developments on this front, such as the creation of the OEWG by Russia in 2018, the promotion of the Code of Conduct for Information Security in 2015, and the organization of the annual WIC. These developments suggest an increase in fragmentation of the global internet governance regime and ongoing attempts of competitive

regime creation and regime shifting. This dissertation has focused much on these contestation processes themselves and the strategies that authoritarian states pursue. Future research should further explore the scope conditions under which competitive regime creation or regime shifting are successful.

This dissertation pointed towards the direction of persuasion strategies such as the securitization of content, but there might be other causal mechanisms that contribute to a successful (or unsuccessful) contestation. For instance, authoritarian norm entrepreneurs try to push decision-making towards intergovernmental institutions such as the UN because they are based on 'one country, one vote' principles (Mueller, 2011, p. 181). Hence, references to democracy and equitable representation might (paradoxically) increase the role of states in content control. Additionally, references to broader principles such as development and stability resonate with developing countries and rising economies, potentially tipping the scale in global internet governance debates.

Third, more research is needed on states that are digital deciders or swing states (Maurer & Morgus, 2014), which are defined as a group of countries that remain largely undecided in global internet governance debates, while at the same time possessing the capacity to influence these debates (Morgus et al., 2018). Digital deciders might affect the outcome of global internet governance debates and norms in the future by supporting either the liberal sphere or the sovereigntist sphere. In Chapter 2, I showed that the proponents of the liberal and sovereigntist spheres of authority are supported by this shifting group of states. It even determined the outcome of the WCIT-12, whereby the sovereigntists' success of convincing a group of digital deciders led to the creation of a competitive ITR regime. In the end, 89 countries (under which many African countries, Arab states, China, Russia, Iran, and emerging economies like Argentina, Brazil, Indonesia, Mexico, South Korea, and Turkey) signed the revised ITRs whereas 55 countries (under which Australia, Canada, EU member states, India, Japan, New Zealand, and the US) did not.

The behavior of digital deciders can be explained in several ways. From a realist perspective, digital deciders are revisionist powers. They would oppose, confront and contest international institutions that stem from a hegemon (Arrighi, 2007; Gilpin, 1981, pp. 23–24; Mearsheimer, 2010; Schweller, 1999; Van der Pijl, 2005, Chapter 3). From a liberal and neoliberal institutionalist perspective, median powers are conformists. They benefit from existing international institutions and have only limited capacity to change them (Jordaan, 2003, pp. 168–169; Kahler, 2013, p. 714). A more middle ground perspective would argue that digital

deciders work within the global internet governance system to demand change in norms, rules, and decision-making procedures (Zürn, 2018, pp. 179–180). In line with this dissertation, they would be enabled and constrained by their regime type. At the same time, they would also attempt to challenge and reorder institutional inequalities that are embedded into the current open internet order. More research is needed into the motivations and behavior of these digital deciders, which have an impact on the future of the open internet order.

IV. Societal implications

The implication of my findings for societal debates and policy-makers is a simple but powerful one: change the tone of debates on content control. If from a liberal democratic perspective, the purpose is to protect freedom of speech online, then content control debates should not be organized in terms of which content we want to control. Instead, it should be held along the lines of which content we find valuable in a liberal democracy and, by extension, which content we want to protect. This also means refraining from securitizing content, because then "the security of the nation-state becomes primary, and the security of end users and private network operators who are communicating globally becomes secondary." (Mueller, 2017, p. 74) Security concerns with regard to content are only justified if that content is actually about security. However, in liberal democracies, security concerns should never become a fig leave for increased content control.

For instance, extensive network interference took place during the 2017 Catalan independence referendum in Spain. Major ISPs blocked websites, targeting civil society websites, communication tools, and information portals (Lundström & Xynou, 2017; Ververis et al., 2021). Ververis et al. show that several state authorities forced ISPs to block content, such as the Spanish Civil Guard, the General Directorate of Police, and the Judicial National Police. And they often did so under pretenses such as enforcing copyright and gambling regulations. Furthermore, Spanish authorities tried to obfuscate their content control practices to make it seem as if web pages were not blocked but rather unreachable (2021). Even though the Spanish Constitutional Court ruled the Catalan independence referendum unconstitutional (Lundström & Xynou, 2017), this does not legitimize nontransparent content control in a liberal democracy. Instead, being transparent about which websites are blocked for which reasons could help reduce over-blocking and unintended blocking (Ververis et al., 2021). If we would go beyond debates on which content should be blocked, transparency could lead to more

accountability. Then, it could even fuel societal debates about which content citizens want to protect.

Another questionable practice from a liberal democratic point of view is the strong reliance of liberal democracies on intermediaries for controlling content. Collaborations between states and private companies take place in regulatory twilight zones (Elkin-Koren & Haber, 2016, pp. 107, 115) that often evade the rule of law and bypass institutional constraints. After all, even if a certain type of content is considered legal, an intermediary can still decide to remove it based on its terms of service (Hintz, 2016, pp. 325–326). Hence, this decentralized intermediary approach is undemocratic and implies an 'outsourcing' (McIntyre, 2013) of internet censorship. Attempts such as the EC Code of Practice on Disinformation and the German Network Enforcement Act impose stricter rules in this domain and are essentially attempts to force intermediaries to comply with government requests. However, they do not solve any of the problems discussed above and often only put extra time pressure on intermediaries to remove content. Instead, there should be more focus on, for instance, the institutional constraints on governments for submitting requests that are within the scope of freedom of speech online, or the rights of internet users to reinstate content that was unjustifiably removed. The open internet order is being contested and if liberal democracies are not there to protect it, the internet will most likely fragment further; incrementally but increasingly resembling national borders. This dissertation has shown the beginning of the end of the open and liberal internet order as we know it.

References

Acharya, A. (2004). How ideas spread: Whose norms matter? Norm localization and institutional change in Asian regionalism. *International Organization*, *58*(2), 239–275.

Acharya, A. (2011). Norm subsidiarity and regional orders: Sovereignty, regionalism, and rule-making in the third world. *International Studies Quarterly*, *55*(1), 95–123.

Adamson, F. B. (2005). Global liberalism versus political Islam: Competing ideological frameworks in international politics. *International Studies Review*, *7*(4), 547–569.

Alden, C., & Large, D. (2015). On becoming a norms maker: Chinese foreign policy, norms evolution and the challenges of security in Africa. *The China Quarterly*, *221*, 123–142.

Algeria, Saudi Arabia, Bahrain, China, United Arab Emirates, Russian Federation, Iraq, & Sudan. (2012). *Proposals for the Work of the Conference, Document 47-E*. http://files.wcitleaks.org/public/S12-WCIT12-C-0047!!MSW-E.pdf

Allison, R. (2008). Virtual regionalism, regional structures and regime security in Central Asia. *Central Asian Survey*, *27*(2), 185–202.

Ambrosio, T. (2008). Catching the 'Shanghai spirit': How the Shanghai Cooperation Organization promotes authoritarian norms in Central Asia. *Europe-Asia Studies*, *60*(8), 1321–1344.

Ambrosio, T. (2010). Constructing a framework of authoritarian diffusion: Concepts, dynamics, and future research. *International Studies Perspectives*, *11*(4), 375–392.

Arrighi, G. (2007). *Adam Smith in Beijing: Lineages of the twenty-first century*. Verso books.

Bak, D., Sriyai, S., & Meserve, S. A. (2018). The internet and state repression: A cross-national analysis of the limits of digital constraint. *Journal of Human Rights*, *17*(5), 642–659.

Baldino, D., & Goold, J. (2014). Iran and the emergence of information and communications technology: The evolution of revolution? *Australian Journal of International Affairs*, *68*(1), 17–35.

Balzacq, T., Léonard, S., & Ruzicka, J. (2016). 'Securitization' revisited: Theory and cases. *International Relations*, *30*(4), 494–531.

Bambauer, D. E. (2009a). Filtering in Oz: Australia's foray into Internet censorship. *University of Pennsylvania Journal of International Law*, *31*(2), 493–530.

Bambauer, D. E. (2009b). Guiding the censor's scissors: A framework to assess Internet filtering. *Brooklyn Law School. Legal Studies Paper*, *149*, 1–72.

Barlow, J. P. (1996, February 8). *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. https://www.eff.org/nl/cyberspace-independence

Beetham, D. (1991). Towards a social-scientific concept of legitimacy. In *The legitimation of power* (pp. 3–41). Springer.

Bingham, P. G. (1982). *Contemporary Democracies: Participation, Stability, and Violence*. Harvard University Press.

Birnhack, M. D., & Elkin-Koren, N. (2003). The invisible handshake: The reemergence of the state in the digital environment. *Virginia Journal of Law & Technology*, *8*(6), 1–57.

Björkdahl, A. (2002). *From Idea to Norm-Promoting Conflict Prevention*. Department of Political Science, Lund University.

Björkdahl, A. (2013). Ideas and norms in Swedish peace policy. *Swiss Political Science Review*, *19*(3), 322–337.

Blanton, S. L., & Blanton, R. G. (2007). What attracts foreign investors? An examination of human rights and foreign direct investment. *The Journal of Politics*, *69*(1), 143–155.

Boas, T. C. (2006). Weaving the authoritarian web: The control of Internet use in nondemocratic regimes. In J. Zysman & A. L. Newman (Eds.), *How Revolutionary Was the Digital Revolution? National Responses, Market Transitions, and Global Technology* (pp. 361–378). Stanford Business Books.

Bob, C. (2012). *The global right wing and the clash of world politics*. Cambridge University Press.

Boyle, J. (1997). Foucault in cyberspace: Surveillance, sovereignty, and hardwired censors. *U. Cin. L. Rev.*, *66*, 177.

Breindl, Y. (2013). *Internet content regulation in liberal democracies. A literature review*. *DH Forschungsverbund – Working Papers zu Digital Humanities*(2). https://www.gcdh.de/fileadmin/user_upload/YBreindl_Literature_Review_Mar2013_final.pdf

Breindl, Y., & Kuellmer, B. (2013). Internet content regulation in France and Germany: Regulatory paths, actor constellations, and policies. *Journal of Information Technology & Politics*, *10*(4), 369–388.

Breindl, Y., Theiner, P., & Busch, A. (2015). Internet blocking regulations: A comparative analysis of 21 liberal democracies. *111th Annual Meeting of the American Political Science Association, San Francisco, CA*.

BRICS. (2014). *Fortaleza Declaration*. http://brics.itamaraty.gov.br/press-releases/214-sixth-brics-summit-fortaleza-declaration

BRICS. (2015). *Ufa Declaration*. https://www.brics2017.org/English/Documents/Summit/201701/t20170125_1409.html

BRICS. (2017). *Xiamen Declaration*. https://timesofindia.indiatimes.com/india/brics-leaders-xiamen-declaration-full-text/articleshow/60359120.cms

Brown, I. (2010). Beware self-regulation. *Index on Censorship*, *39*(1), 98–106.

Busch, A., Theiner, P., & Breindl, Y. (2018). Internet Censorship in Liberal Democracies: Learning from Autocracies? In *Managing democracy in the digital age* (pp. 11–28). Springer.

Busch, M. L. (2007). Overlapping institutions, forum shopping, and dispute settlement in international trade. *International Organization*, *61*(4), 735–761.

Buzan, B., Waever, O., 1960-, & Wilde, J. de. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Cameron, D. R., & Orenstein, M. A. (2012). Post-Soviet Authoritarianism: The Influence of Russia in Its "Near Abroad." *Post-Soviet Affairs*, *28*(1), 1–44.

Cammaerts, B., & Mansell, R. (2020). Digital Platform Policy and Regulation: Toward a Radical Democratic Turn. *International Journal of Communication; Vol 14 (2020)*.

Cavalli, O., & Scholte, J. A. (2021). The role of states in internet governance at ICANN. In *Power and Authority in Internet Governance* (pp. 37–55). Routledge.

Celeste, E. (2019). Digital constitutionalism: A new systematic theorisation. *International Review of Law, Computers & Technology*, *33*(1), 76–99.

Censored Planet. (2019). *Censored Planet*. https://censoredplanet.org/

Chenoweth, E. (2010). Democratic competition and terrorist activity. *The Journal of Politics*, *72*(1), 16–30.

China. (2014a). *An International Code of Conduct for Information Security*. http://www.unidir.ch/files/conferences/pdfs/a-cyber-code-of-conduct-the-best-vehicle-for-progress-en-1-963.pdf

China. (2014b). *Speech by Xi Jinping At the 14th Meeting of the Council of the Heads of State of The SCO Member States*. https://www.fmprc.gov.cn/mfa_eng/topics_665678/zjpcxshzzcygyslshdsschybdtjkstmedfsllkydjxgsfw/t1192339.shtml

China. (2014c). *Statement by Wang Yi, Minister of Foreign Affairs of China, At the General Debate of the 69th Session of The UNGA*. https://www.un.org/en/ga/69/meetings/gadebate/pdf/CN_en.pdf

China. (2015a). *Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference*. https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1242257.shtml

China. (2015b). *Remarks by Xi Jinping President of China At the Opening Ceremony of the Second WIC*. https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml

China. (2017). *International Strategy of Cooperation on Cyberspace*. http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm

China. (2019). *China's Submissions to the OEWG*. https://www.un.org/disarmament/open-ended-working-group/

China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, & Uzbekistan. (2015). *A/69/723. Letter dated 9 January 2015 from the Permanent Representative of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*. https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/Shanghai+Cooperation+Organization+Draft+International+Code+of+Conduct+for+Information+Security+1-13-2015.pdf

China, Russia, Tajikistan, & Uzbekistan. (2011). *A/66/359. Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*. https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/Shanghai+Cooperation+Organization+Draft+International+Code+of+Conduct+for+Information+Security+9-14-2011.pdf

Choucri, N. (2012). *Cyberpolitics in international relations*. MIT press.

Clark, A. M. (2010). *Diplomacy of conscience: Amnesty International and changing human rights norms*. Princeton University Press.

CoE. (2001). *Convention on Cybercrime* (ETS No 185). ETS No 185. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Coleman, K. P. (2013). Locating norm diplomacy: Venue change in international norm negotiations. *European Journal of International Relations*, *19*(1), 163–186.

Conrad, C. R., Hill Jr, D. W., & Moore, W. H. (2018). Torture and the limits of democratic institutions. *Journal of Peace Research*, *55*(1), 3–17.

Coppedge, M., Gerring, J., Knutsen, C. H., Lindberg, S. I., Skaaning, S.-E., Teorell, J., Altman, D., Bernhard, M., Fish, M. S., Cornell, A., Glynn, A., Hicken, A., Lührmann, A., Marquardt, K. L., McMann, K., Paxton, P., Pemstein, D., Seim, B., Sigman, R., … Ziblatt, D. (2019). *V-Dem dataset v9*.

Council of the European Union. (2017). *European Council conclusions on security and defence*. http://www.consilium.europa.eu/en/press/press-releases/2017/06/22/euco-security-defence/

CSTO. (2009, April 15). *Страны ОДКБ проводят широкомасштабную операцию по противодействию киберпреступности*. http://www.odkb-csto.org/archive/news/detail.php?ELEMENT_ID=718&SECTION_ID=92

CSTO. (2011, December 21). *ОДКБ будет активно бороться с киберпреступностью*. http://www.odkb-csto.org/archive/news/detail.php?ELEMENT_ID=558&SECTION_ID=92

CSTO. (2012, April 25). *Тезисы выступления Генерального секретаря ОДКБ Н.Н. Бордюжи на VIII-ой Международной научно-практической конференции*.

CSTO. (2013a, March 26). *Николай Бордюжа в интервью газете "Коммерсантъ": «Есть вещи, которые для нас запретны» Генсек ОДКБ об отношениях с НАТО и о противостоянии внутренним и внешним угрозам*.

CSTO. (2013b, April 18). *Аналитическая Ассоциация ОДКБ Рекомендации Круглого стола на тему "Информация и терроризм."*

CSTO. (2013c, June 7). *Генеральный секретарь ОДКБ Николай Бордюжа принял участие в работе IX Инфофорума-2013 «Евразия-СИТИ» в Москве*. http://www.odkb-csto.org/news/detail.php?ELEMENT_ID=2056&SECTION_ID=91&sphrase_id=53066

CSTO. (2014, July 11). *Аналитическая Ассоциация ОДКБ в первом полугодие 2014 года провела 10 мероприятий, направленных на реализацию основ единой скоординированной политики Организации*. http://www.odkb-csto.org/association/news/detail.php?ELEMENT_ID=3580

CSTO. (2016, May 28). *Николай Бордюжа в интервью МТРК "Мир": Создание единого террористического списка в ОДКБ станет прорывом*.

CSTO. (2018, June 19). *Журнал «Международная жизнь»—Вызовы информационной безопасности и опыт ОДКБ*. http://www.odkb-csto.org/news/detail.php?ELEMENT_ID=12965&SECTION_ID=92

Dahl, R. A. (1956). *A preface to democratic theory*. University of Chicago Press.

Dahl, R. A. (1971). *Polyarchy: Participation and opposition*. Yale University Press.

Dahl, R. A. (1998). *On democracy*. Yale University Press.

Davenport, C. (2004). The promise of democratic pacification: An empirical assessment. *International Studies Quarterly, 48*(3), 539–560.

Davenport, C. (2007a). State repression and political order. *Annual Review Political Science, 10*, 1–23.

Davenport, C. (2007b). *State repression and the domestic democratic peace*. Cambridge University Press.

Davenport, C., & Armstrong, D. A. (2004). Democracy and the violation of human rights: A statistical analysis from 1976 to 1996. *American Journal of Political Science*, *48*(3), 538–554.

Davis, D. W. (2007). *Negative liberty: Public opinion and the terrorist attacks on America*. Russell Sage Foundation.

Davis, D. W., & Silver, B. D. (2004). Civil liberties vs. Security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science*, *48*(1), 28–46.

Daxecker, U. E., & Hess, M. L. (2013). Repression hurts: Coercive government responses and the demise of terrorist campaigns. *British Journal of Political Science*, *43*(3), 559–577.

De Mesquita, B. B., Downs, G. W., Smith, A., & Cherif, F. M. (2005). Thinking inside the box: A closer look at democracy and human rights. *International Studies Quarterly*, *49*(3), 439–457.

Debre, M. (2018). *Autocracy from the Outside-In? The Role of Regional Organizations in Boosting Authoritarian Resilience*. Freie Universität Berlin.

Deibert, R. J., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance: A Review of Multilateralism and International Organizations*, *18*(3), 339–361.

Deibert, R. J., Palfrey, J., Rohozinski, R., & Zittrain, J. (2012). *Access Contested. Security, Identity and Resistance in Asian Cyberspace* (R. J. Deibert, R. Rohozinski, & J. Zittrain, Eds.). MIT Press.

Deibert, R. J., Palfrey, J., Rohozinski, R., Zittrain, J., & OpenNet Initiative (Eds.). (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. MIT Press.

Deibert, R. J., Palfrey, J., Rohozinski, R., Zittrain, J., & Stein, J. G. (2008). *Access denied: The practice and policy of global internet filtering*. MIT Press.

Deibert, R. J., & Rohozinski, R. (2010). Liberation vs. Control: The future of cyberspace. *Journal of Democracy*, *21*(4), 43–57.

Delerue, F. (2018). *ESIL Reflection: The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC? 7*(4). http://esil-sedi.eu/?p=12815

Demchak, C. C., & Dombrowski, P. (2011). Rise of a cybered westphalian age. *Strategic Studies Quarterly*, *5*(1), 32–61.

DeNardis, L. (2012). Hidden Levers of Internet Control. An Infrastructure-based Theory of Internet Governance. *Information, Communication & Society*, *15*(5), 720–738.

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

Diamond, L. (2002). Elections without democracy: Thinking about hybrid regimes. *Journal of Democracy*, *13*(2), 21–35.

Diamond, L. (2010). Liberation Technology. *Journal of Democracy*, *21*(3), 69–83.

Diamond, L., & Plattner, M. F. (2012). *Liberation technology: Social media and the struggle for democracy*. JHU Press.

Dick, A. L., Oyieke, L. I., & Bothma, T. J. (2012). Are established democracies less vulnerable to Internet censorship than authoritarian regimes? The social media test. *FAIFE Spotlight*.

Dingwerth, K., Schmidtke, H., Weise, T., & Wodarz, J. (2015, April 29). *Speaking democracy: Why international organizations adopt a democratic rhetoric*. ECPR Joint Sessions, Warsaw.

Drake, W. J., Cerf, V. G., & Kleinwächter, W. (2016). Internet Fragmentation: An Overview. *Future of the Internet Initiative White Paper*.

Drezner, D. W. (2004). The global governance of the internet: Bringing the state back in. *Political Science Quarterly*, *119*(3), 477–498.

Drezner, D. W. (2007). *All Politics Is Global: Explaining International Regulatory Regimes*. Princeton University Press.

Easton, D. (1965). *A systems analysis of political life*. Wiley.

Ebert, H., & Maurer, T. (2013). Contested cyberspace and rising powers. *Third World Quarterly*, *34*(6), 1054–1074.

EC. (2005). *Press release—Commission outlines EU negotiation principles for the World Summit on the Information Society in Tunis* (IP/05/672). http://europa.eu/rapid/press-release_IP-05-672_en.htm?locale=en

EC. (2018a). *A Europe that protects: Countering illegal content online*. https://ec.europa.eu/digital-single-market/en/news/europe-protects-countering-illegal-content-online

EC. (2018b). *Action Plan against Disinformation*. https://eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf

EC. (2019). *Tackling online disinformation*. https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation

Eichensehr, K. E. (2018). Digital Switzerlands. *University of Pennsylvania Law Review*, *167*, 665.

Elkin-Koren, N., & Haber, E. (2016). Governance by Proxy: Cyber Challenges to Civil Liberties. *Brooklyn Law Review*, *82*, 105–164.

Escribà-Folch, A. (2013). Repression, political threats, and survival under autocracy. *International Political Science Review*, *34*(5), 543–560.

Faris, R., & Villeneuve, N. (2008). Measuring global Internet filtering. *Access Denied: The Practice and Policy of Global Internet Filtering*, *5*.

Farrell, H., & Newman, A. L. (2018). Linkage Politics and Complex Governance in Transatlantic Surveillance. *World Politics*, *70*(4), 515–554.

Farrell, H., & Newman, A. L. (2019). *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security*. Princeton University Press.

Farrell, H., & Newman, A. L. (2021). The Janus Face of the Liberal International Information Order: When Global Institutions Are Self-Undermining. *International Organization*, 1–26. Cambridge Core.

Fein, H. (1995). Life-integrity Violations and Democracy in the World, 1987. *Human Rights Quarterly*, *17*(1), 170–191.

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, *110*(3), 425–479.

Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization*, *52*(4), 887–917.

Fischer-Lescano, A. (2016). Struggles for a global Internet constitution: Protecting global communication structures against surveillance measures. *Global Constitutionalism*, *5*(2), 145–172.

Fishman, R. M. (1990). Rethinking state and regime: Southern Europe's transition to democracy. *World Politics*, *42*(3), 422–440.

Flonk, D., Jachtenfuchs, M., & Obendiek, A. S. (2020). Authority conflicts in internet governance: Liberals vs. Sovereigntists? *Global Constitutionalism*, *9*(2), 364–386.

Florini, A. (1996). The evolution of international norms. *International Studies Quarterly*, *40*(3), 363–389.

Freyburg, T., & Garbe, L. (2018). Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa. *International Journal of Communication*, *12*, 3896–3916.

Frosio, G. F. (2018). Why keep a dog and bark yourself? From intermediary liability to responsibility. *International Journal of Law and Information Technology*, *26*(1), 1–33.

Gandhi, J., & Lust-Okar, E. (2009). Elections under authoritarianism. *Annual Review of Political Science*, *12*, 403–422.

Geddes, B., Wright, J., & Frantz, E. (2014). Autocratic breakdown and regime transitions: A new data set. *Perspectives on Politics*, 313–331.

Geier, K. (2018). *Podcast: Cyberspace, international norms, and a new initiative in the UN?* https://www.nupi.no/en/News/PODCAST-Cyberspace-international-norms-and-a-new-initiative-in-the-UN

Gholiagha, S., Holzscheiter, A., & Liese, A. (2020). Activating norm collisions: Interface conflicts in international drug control. *Global Constitutionalism*, *9*(2), 290–317. Cambridge Core.

Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.

Gilpin, R. (1981). *War and change in world politics*. Cambridge University Press.

Global Times. (2014, June 9). *SCO takes on challenge of trans-border terror*. https://www.globaltimes.cn/content/864630.shtml

Goldsmith, J. L., & Wu, T. (2006). *Who Controls the Internet?: Illusions of a Borderless World*. Oxford University Press.

Goldstein, R. J. (2001). *Political repression in modern America from 1870 to 1976*. University of Illinois Press.

Golkar, S. (2011). Liberation or suppression technologies? The Internet, the Green Movement and the regime in Iran. *International Journal of Emerging Technologies and Society*, *9*(1), 50.

Gomez, J. (n.d.). Dumbing down democracy: Trends in internet regulation, surveillance and control in Asia. *Pacific Journalism Review*, *2*(10), 130–150.

Goodman, R., & Jinks, D. (2013). *Socializing states: Promoting human rights through international law*. Oxford University Press.

Google. (2019). *Government request to remove content*. https://transparencyreport.google.com/government-removals/overview

Grigorescu, A. (2010). The Spread of Bureaucratic Oversight Mechanisms across Intergovernmental Organizations1. *International Studies Quarterly*, *54*(3), 871–886.

Hafner-Burton, E. M. (2005). Trading human rights: How preferential trade agreements influence government repression. *International Organization*, *59*(3), 593–629.

Haggart, B., Tusikov, N., & Scholte, J. A. (2021). *Power and Authority in Internet Governance: Return of the State?* Routledge.

Han, R. (2015). Defending the Authoritarian Regime Online: China's" Voluntary Fifty-cent Army". *The China Quarterly*, 1006–1025.

Harwit, E., & Clark, D. (2001). Shaping the internet in China. Evolution of political control over network infrastructure and content. *Asian Survey*, *41*(3), 377–408.

Hellmeier, S. (2016). The Dictator's Digital Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes. *Politics & Policy*, *44*(6), 1158–1191.

Henderson, C. W. (1993). Population pressures and political repression. *Social Science Quarterly*, *74*(2), 322–333.

Heydemann, S., & Leenders, R. (2011). Authoritarian learning and authoritarian resilience: Regime responses to the 'Arab Awakening.' *Globalizations*, *8*(5), 647–653.

Hill, R. (2013). WCIT: failure or success, impasse or way forward? *International Journal of Law and Information Technology*, *21*(3), 313–328.

Hintz, A. (2016). Restricting digital sites of dissent: Commercial social media and free expression. *Critical Discourse Studies*, *13*(3), 325–340.

Hintz, A., & Milan, S. (2018a). Authoritarian Practices in the Digital Age|"Through a Glass, Darkly": Everyday Acts of Authoritarianism in the Liberal West. *International Journal of Communication*, *12*, 21.

Hintz, A., & Milan, S. (2018b). Through a Glass, Darkly: Everyday Acts of Authoritarianism in the Liberal West. *International Journal of Communication*, *12*, 3939–3959.

Ho, S. (2020). Infrastructure and Chinese power. *International Affairs*, *96*(6), 1461–1485.

Hofmann, J. (2005). Internet Governance: Zwischen staatlicher Autorität und privater Koordination. *Internationale Politik Und Gesellschaft*, *3*(2005), 10–39.

Hofmann, J., Katzenbach, C., & Gollatz, K. (2017). Between coordination and regulation: Finding the governance in Internet governance. *New Media & Society*, *19*(9), 1406–1423.

Hofstetter, H., Dusseldorp, E., Zeileis, A., & Schuller, A. A. (2016). Modeling caries experience: Advantages of the use of the hurdle model. *Caries Research*, *50*(6), 517–526.

Hurwitz, R. (2014). The play of states: Norms and security in cyberspace. *American Foreign Policy Interests*, *36*(5), 322–331.

Ikenberry, G. J. (2018). The end of liberal international order? *International Affairs*, *94*(1), 7–23.

ITU. (1988). *ITRs*. https://www.itu.int/osg/spuold/wtpf/wtpf2009/documents/ITU_ITRs_88.pdf

ITU. (2012a). *Final Acts of the WCIT*. https://www.itu.int/pub/S-CONF-WCIT

ITU. (2012b). *Signatories of the Final Acts: 89*. https://www.itu.int/osg/wcit-12/highlights/signatories.html

ITU. (2019). *Individuals using the Internet (% of population)*. https://data.worldbank.org/indicator/IT.NET.USER.ZS

Jordaan, E. (2003). The concept of a middle power in international relations: Distinguishing between emerging and traditional middle powers. *Politikon*, *30*(1), 165–181.

Jose, B. (2017). *Norm Contestation: Insights Into Non-Conformity with Armed Conflict Norms*. Springer.

Jose, B., & Stefes, C. H. (2018). Russian norm entrepreneurship in Crimea: Serious contestation or cheap talk? *GIGA Working Paper*, *311*. https://www.giga-hamburg.de/en/system/files/publications/wp311_jose-stefes.pdf

Ju, H. (2005, November 17). *Statement by Vice Premier Huang Ju, The State Council of The People's Republic of China*. WSIS, Tunis. https://www.itu.int/net/wsis/tunis/statements/docs/g-china/1.html

Kahler, M. (2013). Rising powers and global governance: Negotiating change in a resilient status quo. *International Affairs*, *89*(3), 711–729.

Kalathil, S., & Boas, T. (2003). *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Carnegie Endowment. https://carnegieendowment.org/2003/01/18/open-networks-closed-regimes-impact-of-internet-on-authoritarian-rule-pub-1072

Kaufmann, D., Kraay, A., & Mastruzzi, M. (2011). The worldwide governance indicators: Methodology and analytical issues. *Hague Journal on the Rule of Law*, *3*(2), 220–246.

Keck, M. E., & Sikkink, K. (2014). *Activists beyond borders: Advocacy networks in international politics*. Cornell University Press.

Keith, L. C. (2002). Constitutional provisions for individual human rights (1977-1996): Are they more than mere "window dressing?" *Political Research Quarterly*, *55*(1), 111–143.

Keohane, R. (2011). Neoliberal institutionalism. In C. W. Hughes & L. Y. Meng (Eds.), *Security studies: A reader* (pp. 157–164). Routledge.

Kerr, J. (2014). The Digital Dictator's Dilemma: Internet Regulation and Political Control in Non-Democratic States, presentado en Social Science Seminar Series. *The Center for International Security and Cooperation (CISAC), Stanford University, October*, *16*, 2014.

Kierkegaard, S. M. (2007). EU tackles cybercrime. In *Cyber warfare and cyber terrorism* (pp. 431–438). IGI Global.

King, G., Pan, J., & Roberts, M. E. (2013a). How censorship in China allows government criticism but silences collective expression. *American Political Science Review*, *107*(2), 326–343.

King, G., Pan, J., & Roberts, M. E. (2013b). How Censorship in China Allows Government Criticism but Silences Collective Expression. *American Political Science Review*, *107*(2), 326–343.

Kleinwächter, W. (2004). Beyond ICANN Vs ITU? How WSIS tries to enter the new territory of Internet governance. *Gazette (Leiden, Netherlands)*, *66*(3–4), 233–251.

Knutsen, C. H., Nygård, H. M., & Wig, T. (2017). Autocratic Elections: Stabilizing Tool or Force for Change? *World Politics*, *69*(1), 98–143. Cambridge Core.

Kreuder-Sonnen, C., & Zürn, M. (2020). After fragmentation: Norm collisions, interface conflicts, and conflict management. *Global Constitutionalism*, *9*(2), 241–267. Cambridge Core.

Krisch, N., Corradini, F., & Reimers, L. L. (2020). Order at the margins: The legal construction of interface conflicts over time. *Global Constitutionalism*, *9*(2), 343–363. Cambridge Core.

Krueger, B. S. (2006). A comparison of conventional and Internet political mobilization. *American Politics Research*, *34*(6), 759–776.

Kuran, T. (1997). *Private truths, public lies: The social consequences of preference falsification*. Harvard University Press.

LaFree, G., & Tseloni, A. (2006). Democracy and crime: A multilevel analysis of homicide trends in forty-four countries, 1950-2000. *The Annals of the American Academy of Political and Social Science*, *605*(1), 25–49.

Lavrov, S. (2017). *Statement by Foreign Minister Sergey Lavrov at the 72nd session of the UN General Assembly*. United Nations. http://www.mid.ru/en/vizity-ministra/-/asset_publisher/ICoYBGcCUgTR/content/id/2870898

Lessig, L. (2000). Code is law. *Harvard Magazine*, *2000*. https://www.harvardmagazine.com/2000/01/code-is-law-html

Levitsky, S., & Way, L. A. (2010). *Competitive authoritarianism: Hybrid regimes after the Cold War*. Cambridge University Press.

Lindberg, S. I. (2009). Democratization by elections? A mixed record. *Journal of Democracy*, *20*(3), 86–92.

Lucchi, N. (2013). Internet content governance and human rights. *Vanderbilt Journal of Entertainment and Technology Law*, *16*(4), 809–856.

Lührmann, A., Tannenberg, M., & Lindberg, S. I. (2018). Regimes of the World (RoW): Opening New Avenues for the Comparative Study of Political Regimes. *Politics & Governance*, *6*(1).

Lundström, T., & Xynou, M. (2017, October 3). *Evidence of Internet Censorship during Catalonia's Independence Referendum*. https://ooni.org/post/internet-censorship-catalonia-independence-referendum/

MacKinnon, R. (2013). *Consent of the networked: The world-wide struggle for Internet freedom*. Basic Books.

Mailland, J. (2000). Freedom of speech, the internet, and the costs of control: The French example. *New York Universtiy Journal of International Law & Politics*, *33*, 1179.

Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. *Media and Communication*, *5*(1).

Markoff, M. G. (2017). *Explanation of Position at the Conclusion of the 2016-2017 UN GGE*. https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm

Mathiason, J. (2008). *Internet governance: The new frontier of global institutions*. Routledge.

Maurer, T., & Morgus, R. (2014). *Tipping the scale: An analysis of global swing states in the internet governance debate* (No. 7). CIGI Internet Governance Papers.

McIntyre, T. J. (2013). Child abuse images and cleanfeeds: Assessing internet blocking systems. *Research Handbook on Governance of the Internet*, 277–308.

Mearsheimer, J. J. (2010). The gathering storm: China's challenge to US power in Asia. *The Chinese Journal of International Politics*, *3*(4), 381–396.

Merkel, W. (2004). Embedded and defective democracies. *Democratization*, *11*(5), 33–58.

Meserve, S. (2018). Why Do Governments Censor? Expanding from State Survival to Content Regulation Theories in Political Science. *Comparative Politics Newsletter*, 55–59.

Meserve, S., & Pemstein, D. (2018). Google politics: The political determinants of Internet censorship in democracies. *Political Science Research and Methods*, *6*(2), 245–263.

Michaelsen, M., & Glasius, M. (2018). Authoritarian Practices in the Digital Age—Introduction. *International Journal of Communication*, *12*, 7.

Moe, L. W., & Geis, A. (2020). From liberal interventionism to stabilisation: A new consensus on norm-downsizing in interventions in Africa. *Global Constitutionalism*, *9*(2), 387–412. Cambridge Core.

Moravcsik, A. (1997). Taking Preferences Seriously: A Liberal Theory of International Politics. *International Organization*, *51*(4), 513–553.

Morgus, R., Woolbright, J., & Sherman, J. (2018). *The Digital Deciders: How a group of often overlooked countries could hold the keys to the future of the global internet*. https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/

Morozov, E. (2011). *The net delusion: How not to liberate the world*. Penguin UK.

Morse, J. C., & Keohane, R. O. (2014). Contested multilateralism. *The Review of International Organizations*, *9*(4), 385–412.

Mueller, M. (2010). *Networks and states: The global politics of Internet governance*. Cambridge, Mass.: MIT Press.

Mueller, M. (2011). China and global Internet governance: A tiger by the tail. In R. J. Deibert, J. Palfrey, & J. Zittrain (Eds.), *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (pp. 177–194). MIT Press.

Mueller, M. (2017). *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. John Wiley & Sons.

Mueller, M., Mathiason, J., & Klein, H. (2007). The Internet and global governance: Principles and norms for a new regime. *Global Governance: A Review of Multilateralism and International Organizations*, *13*(2), 237–254.

Muller, H., & Wunderlich, C. (2013). *Norm dynamics in multilateral arms control: Interests, conflicts, and justice*. University of Georgia Press.

Murdie, A. (2014). *Help or harm: The human security effects of international NGOs*. Stanford University Press.

Murdoch, S. J., & Anderson, R. (2008). Tools and technology of internet filtering. *Access Denied: The Practice and Policy of Global Internet Filtering*, *1*(1), 58.

National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2018). *Global Terrorism Database [Data file]*. https://www.start.umd.edu/gtd

Nisbet, E. C., Stoycheff, E., & Pearce, K. E. (2012). Internet use and democratic demands: A multinational, multilevel model of Internet use and citizen attitudes about democracy. *Journal of Communication*, *62*(2), 249–265.

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, *91*(1), 111–130.

Nye, J. S. (2014). *The Regime Complex for Managing Global Cyber Activities*.

Obendiek, A. S. (2021). *Data Disputes: Jurisdictional Conflicts and the Common Good in the Field of Data Governance*. Hertie School.

OONI. (2019). *Open Observatory of Network Interference*. https://ooni.torproject.org/

OpenNet Initiative. (n.d.). *Country Profiles*. Retrieved January 28, 2020, from https://opennet.net/country-profiles

OpenNet Initiative. (2012). *Global Internet Filtering Map*. https://onimap.citizenlab.org/filtering-pol.html

Organizing Committee for the WIC. (2016). *Wuzhen Report on World Internet Development 2016*. http://www.wuzhenwic.org/2016-11/18/c_61834.htm

Palfrey, J. (2010). Four Phases of Internet Regulation. *Social Research, 77*(3), 981–996.

Patrick, S. M., & Feng, A. (2018, July 2). *Belt and Router: China Aims for Tighter Internet Controls with Digital Silk Road*. Council on Foreign Relations. https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road

Payne, R. A. (2001). Persuasion, frames and norm construction. *European Journal of International Relations*, *7*(1), 37–61.

Pearce, K. E., & Kendzior, S. (2012). Networked authoritarianism and social media in Azerbaijan. *Journal of Communication*, *62*(2), 283–298.

Pearce, P., Ensafi, R., Li, F., Feamster, N., & Paxson, V. (2017). Augur: Internet-wide detection of connectivity disruptions. *2017 IEEE Symposium on Security and Privacy*, 427–443.

Pernice, I. (2018). Global cybersecurity governance: A constitutionalist analysis. *Global Constitutionalism*, *7*(1), 112–141.

Pfanner, E. (2012, December 13). Citing Internet Standoff, U.S. Rejects International Telecommunications Treaty. *The New York Times*. https://www.nytimes.com/2012/12/14/technology/14iht-treaty14.html

Poe, S. C., Tate, C. N., & Keith, L. C. (1999). Repression of the human right to personal integrity revisited: A global cross-national study covering the years 1976–1993. *International Studies Quarterly*, *43*(2), 291–313.

Polatin-Reuben, D., & Wright, J. (2014). An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. *4th USENIX Workshop on Free and Open Communications on the Internet*.

Polyakova, A., & Meserole, C. (2019). *Exporting digital authoritarianism: The Russian and Chinese models* (Democracy and Disorder Series, pp. 1–22). Brookings.

Postmes, T., & Brunsting, S. (2002). Collective action in the age of the Internet: Mass communication and online mobilization. *Social Science Computer Review*, *20*(3), 290–301.

Powers, S. M., & Jablonski, M. (2015). *The real cyber war: The political economy of internet freedom*. University of Illinois Press.

Przeworski, A., Alvarez, R. M., Alvarez, M. E., Cheibub, J. A., & Limongi, F. (2000). *Democracy and development: Political institutions and well-being in the world, 1950-1990* (Vol. 3). Cambridge University Press.

Radsch, C. C. (forthcoming). *The Social Media Front: On the Frontlines of the Information Wars: How Algorithmic Gatekeepers and National Security Impact Journalism*.

Regan, P. M., & Henderson, E. A. (2002). Democracy, threats and political repression in developing countries: Are democracies internally less violent? *Third World Quarterly, 23*(1), 119–136.

Richards, D. L., Gelleny, R. D., & Sacko, D. H. (2001). Money with a mean streak? Foreign economic penetration and government respect for human rights in developing countries. *International Studies Quarterly, 45*(2), 219–239.

Risse-Kappen, T. (2016). Collective Identity in a Democratic Community: The Case of NATO. In *Domestic politics and norm diffusion in international relations: Ideas do not float freely*. Taylor & Francis.

Risse-Kappen, T., Ropp, S. C., & Sikkink, K. (1999). *The power of human rights: International norms and domestic change*. Cambridge University Press.

Roberts, M. E. (2018). *Censored: Distraction and diversion inside China's Great Firewall*. Princeton University Press.

Rød, E. G., & Weidmann, N. B. (2015). Empowering activists or autocrats? The Internet in authoritarian regimes. *Journal of Peace Research, 52*(3), 338–351.

Rodan, G. (1998). The Internet and political control in Singapore. *Political Science Quarterly, 113*(1), 63–89.

Rodan, G. (2004). *Transparency and authoritarian rule in Southeast Asia: Singapore and Malaysia*. Routledge.

Rodríguez, M. (2017). *Declaration by Miguel Rodríguez, Representative of Cuba*. https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf

Ruggiero, S. M. (2011). Killing the Internet to keep America alive: The myths and realities of the Internet kill switch. *SMU Science & Technology Law Review, 15*, 241.

Russia. (2011). *Comment by Russian MFA Spokesman Alexander Lukashevich Regarding Consideration in US Congress of New Global Online Freedom Act*.

Russia. (2013). *Statement by Russian President Vladimir Putin after the Plenary Session of the 5th BRICS Summit*. http://www.brics.utoronto.ca/docs/130327-putin-statement.html

Russia. (2014a). *Interview of the Russian Foreign Minister Sergey Lavrov to China Daily*. http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/65422

Russia. (2014b). *Press statement on the Russian-Chinese Interagency Consultations on international Information Security*. https://www.rusemb.org.uk/foreignpolicy/2643

Russia. (2015a). *Foreign Minister Sergey Lavrov's remarks at the High-Level Conference on Security and Stability in the SCO Region*. http://www.mid.ru/en/web/guest/sanhajskaa-organizacia-sotrudnicestva-sos-/-/asset_publisher/0vP3hQoCPRg5/content/id/1385493

Russia. (2015b). *Comment by the Information and Press Department on Foreign Minister Sergey Lavrov's participation in the 70th Session of the UNGA*. http://www.mid.ru/en/web/guest/general_assembly/-/asset_publisher/lrzZMhfoyRUj/content/id/1793759

Russia. (2017). *Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh*. http://www.mid.ru/en/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/2804288

Russian Federation. (2011). *Convention on International Information Security*. http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

Russian Federation. (2017). *Response to TASS' Question Concerning the State of International Dialogue in This Sphere*. http://www.mid.ru/en/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/2804288

Russian Federation, UAE, China, Saudi Arabia, Algeria, Sudan, & Egypt. (2012). *Proposals for the Work of the Conference, Document DT-X*. http://files.wcitleaks.org/public/Merged%20UAE%20081212.pdf

Sarikakis, K. (2012). Securitization and legitimacy in global media governance. In I. Volkmer (Ed.), *The handbook of global media research* (pp. 143–155). Wiley-Blackwell.

Schedler, A. (2013). *The politics of uncertainty: Sustaining and subverting electoral authoritarianism*. Oxford University Press.

Schlumberger, O. (2010). Opening old bottles in search of new wine: On nondemocratic legitimacy in the Middle East. *Middle East Critique*, *19*(3), 233–250.

Scholte, J. A. (2017). Polycentrism and democracy in internet governance. In U. Kohl (Ed.), *The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance* (pp. 165–184). Cambridge University Press.

Scholte, J. A. (2018). *Complex Hegemony. The IANA Transition Global Internet Governance*. ECPR General Conference, Hamburg, Germany.

Schünemann, W. J., & Kneuer, M. (2021). *Do not disturb! Studying discourses of democratic sovereignty as potential drivers of Internet fragmentation through online control*. ISA Annual Convention, Las Vegas, United States.

Schweller, R. (1999). Managing the rise of great powers: History and theory. In *Engaging China: The management of an emerging power* (pp. 1–31). Routledge.

SCO. (2002). *Agreement on RATS between the Member States of the SCO*. http://eng.sectsco.org/documents/

SCO. (2009). *Agreement on Cooperation in Ensuring International Information Security between the Member States of the SCO*. http://eng.sectsco.org/documents/

SCO. (2012a). *Declaration by the Heads of State of the Member States of the SCO on Building a Region of Lasting Peace and Common Prosperity*. http://eng.sectsco.org/documents/

SCO. (2012b). *Press Release of the Meeting of the Council of The Heads of the Member States of The SCO*. http://eng.sectsco.org/documents/

SCO. (2013). *Bishkek Declaration*. http://eng.sectsco.org/documents/

SCO. (2014a). *Press Release Meeting of the Ministers of Foreign Affairs of the Member States of the SCO*. http://eng.sectsco.org/documents/

SCO. (2014b). *Press Release Meeting of the Council of Heads of Member States of the SCO*. http://eng.sectsco.org/documents/

SCO. (2015). *Press Release Meeting of the Council of Heads of Member States of the SCO*. http://eng.sectsco.org/documents/

SCO. (2016a). *Press Communiqué of the Meeting of the Council of Foreign Ministers of the Member States of the SCO*. https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t1366868.shtml

SCO. (2016b). *Press release following a meeting of the SCO Heads of State Council*. http://eng.sectsco.org/documents/

SCO. (2017). *Astana Declaration*. http://eng.sectsco.org/documents/

SCO. (2018). *Qingdao Declaration*. http://eng.sectsco.org/documents/

Segal, A. (2017). Chinese Cyber Diplomacy in a New Era of Uncertainty. *Aegis Paper Series, 1703*.

Sil, R. (2000). The foundations of eclecticism: The epistemological status of agency, culture, and structure in social theory. *Journal of Theoretical Politics, 12*(3), 353–387.

Sil, R., & Katzenstein, P. J. (2010). Analytic eclecticism in the study of world politics: Reconfiguring problems and mechanisms across research traditions. *Perspectives on Politics, 8*(2), 411–431.

Stadnik, I. (2021). Russia: An Independent and Sovereign Internet? In *Power and Authority in Internet Governance: Return of the State?* (pp. 147–167). Taylor & Francis.

Stier, S. (2015). Democracy, autocracy and the news: The impact of regime type on media freedom. *Democratization, 22*(7), 1273–1295.

Stimmer, A., & Wisken, L. (2019). The dynamics of dissent: When actions are louder than words. *International Affairs, 95*(3), 515–533.

Stoycheff, E., Burgess, G. S., & Martucci, M. C. (2018). Online censorship and digital surveillance: The relationship between suppression technologies and democratization across countries. *Information, Communication & Society, 23*(4), 474–490.

Stryker, S., & Statham, A. (1985). Symbolic interaction and role theory. In L. Gardner & E. Aronson (Eds.), *Handbook of social psychology* (pp. 311–378). Random House.

Sukumar, A. M. (2017, July 4). *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?* Lawfare. https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well

Sunstein, C. R. (1996). Social norms and social roles. *Columbia Law Review, 96*(4), 903–968.

Svolik, M. W. (2012). *The politics of authoritarian rule*. Cambridge University Press.

Tallberg, J., Lundgren, M., Sommerer, T., & Squatrito, T. (2020). Why international organizations commit to liberal norms. *International Studies Quarterly, 64*(3), 626–640.

Tallberg, J., Sommerer, T., & Squatrito, T. (2016). Democratic memberships in international organizations: Sources of institutional design. *The Review of International Organizations, 11*(1), 59–87.

Tansey, O. (2016). *International politics of authoritarian rule*. Oxford University Press.

Taureck, R. (2006). Securitization theory and securitization studies. *Journal of International Relations and Development, 9*(1), 53–61.

T-CY. (2017). *Bureau Meeting report* (T-CY (2017)22). Council of Europe. https://rm.coe.int/t-cy-2017-22-bu-meeting-report-sep2017/1680760eaf

The Moscow Times. (2014, April 18). *China Calls on Russia to Tighten Internet Control to Keep Out "External Forces."* The Moscow Times. https://www.themoscowtimes.com/2014/04/18/china-calls-on-russia-to-tighten-internet-control-to-keep-out-external-forces-a34195

Theys, S., & Rietig, K. (2020). The influence of small states: How Bhutan succeeds in influencing global sustainability governance. *International Affairs*, *96*(6), 1603–1622.

Tikk, E., & Kerttunen, M. (2017). *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*. Cyber Policy Institute.

Tréguer, F. (2016). *Internet Surveillance in France's Intelligence Act*. https://halshs.archives-ouvertes.fr/halshs-01399548

Tropina, T., & Callanan, C. (2015). *Self-and co-regulation in cybercrime, cybersecurity and national security*. Springer.

Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From liberation to turmoil: Social media and democracy. *Journal of Democracy*, *28*(4), 46–59.

UNGA. (2013). *A/68/98. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. https://undocs.org/A/68/98

UNGA. (2015a). *A/70/174. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. https://undocs.org/A/70/174

UNGA. (2015b). *A/RES/70/237. Resolution adopted by the GA on 23 December 2015*. https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/01/A-RES-70-237-Information-Security.pdf

UNGA. (2016). *GA/DIS/3560. Calling for Norms to Stymie Cyberattacks, First Committee Speakers Say States Must Work Together in Preventing Information Arms Race*. https://www.un.org/press/en/2016/gadis3560.doc.htm

UNGA. (2017a). *A/RES/71/190. Promotion of a democratic and equitable international order*. adopted by the General Assembly, 9 February 2017. http://undocs.org/A/RES/71/190

UNGA. (2017b). *A/72/327. Report of the GGE*. http://digitallibrary.un.org/record/1301308/files/A_72_327-EN.pdf

UNGA. (2018a). *A/C.3/73/L.9/Rev.1*. Countering the Use of Information and Communications Technologies for Criminal Purposes*. http://undocs.org/A/C.3/73/L.9/Rev.1>

UNGA. (2018b). *A/C.1/73/L.37. Advancing responsible State behaviour in cyberspace in the context of international security*. http://undocs.org/A/C.1/73/L.37

UNGA. (2018c). *A/C.1/73/L.27/Rev.1. Developments in the field of information and telecommunications in the context of international security*. http://undocs.org/A/C.1/73/L.27/Rev.1

United Nations Population Division, National statistical offices, Eurostat, United Nations Statistical Division, U.S. Census Bureau, & Secretariat of the Pacific Community. (2019). *Population, total*. https://data.worldbank.org/indicator/SP.POP.TOTL

US Department of State. (2018). *Explanation of Vote on a Third Committee Resolution on Countering the use of information and communication technologies for criminal purposes*. Bureau of Public Affairs. http://www.state.gov/misc/415.htm/remarks/8803

US Majority Committee Staff. (2012). *Hearing on International Proposals to Regulate the Internet*. https://www.govinfo.gov/content/pkg/CHRG-112hhrg79558/html/CHRG-112hhrg79558.htm

Van der Pijl, K. (2005). *Transnational classes and international relations*. Routledge.

Verveer, P. (2012). *Testimony, Hearing on International Proposals to Regulate the Internet*. https://www.govinfo.gov/content/pkg/CHRG-112hhrg79558/html/CHRG-112hhrg79558.htm

Ververis, V., Ermakova, T., Isaakidis, M., Basso, S., Fabian, B., & Milan, S. (2021). Understanding Internet Censorship in Europe: The Case of Spain. *13th ACM Web Science Conference 2021*, 319–328.

Ververis, V., Marguel, S., & Fabian, B. (2020). Cross-Country Comparison of Internet Censorship: A Literature Review. *Policy & Internet*, *12*(4), 450–473.

Von Soest, C. (2015). Democracy prevention: The international collaboration of authoritarian regimes. *European Journal of Political Research*, *54*(4), 623–638.

Von Soest, C., & Grauvogel, J. (2017). Identity, procedures and performance: How authoritarian regimes legitimize their rule. *Contemporary Politics*, *23*(3), 287–305.

Wacker, G. (2003). The Internet and censorship in China: Gudrun Wacker. In *China and the Internet* (pp. 70–94). Routledge.

Wæver, O. (2004). *Aberystwyth, Paris, Copenhagen: New schools in security theory and their origins between core and periphery*. ISA Annual Convention.

Wagner, B. (2014). The politics of internet filtering: The United Kingdom and Germany in a comparative perspective. *Politics*, *34*(1), 58–71.

Wahl-Jorgensen, K., Bennet, L., & Taylor, G. (2017). The normalisation of surveillance: The invisibility of citizens and their rights in media coverage of the Snowden revelations. *International Journal of Communication*, *11*, 740–762.

Warf, B. (2011). Geographies of global Internet censorship. *GeoJournal*, *76*(1), 1–23.

Weidmann, N. B., & Rød, E. G. (2019). *The Internet and political protest in autocracies.* Oxford Studies in Digital Politics.

Weinberg, J. (2011). Governments, Privatization, and Privatization: ICANN and the GAC. *Michigan Telecommunications & Technology Law Review*, *18*, 189.

Wiener, A. (2014). *A theory of contestation*. Springer.

World Bank, & OECD. (2019). *GDP per capita (constant 2010 US$)*. https://data.worldbank.org/indicator/NY.GDP.PCAP.KD

Wright, J., & Breindl, Y. (2013). Internet filtering trends in liberal democracies: French and German regulatory debates. *Internet Policy Review: Journal on Internet Regulation*, *2*(2), 1–10.

Wright, T. (2005, September 30). EU Tries to Unblock Internet Impasse—New York Times. *The New York Times*. https://archive.nytimes.com/www.nytimes.com/iht/2005/09/30/business/IHT-30net.html?emc=th&th

WSIS. (2005). *WSIS-05/TUNIS/DOC/6(Rev. 1)-E Tunis Agenda for the Information Society*. World Summit on the Information Society, UN, ITU. http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

Wunderlich, C. (2014). A ‘rogue’ gone norm entrepreneurial? Iran within the nuclear nonproliferation regime. In W. Wagner, W. Werner, & M. Onderco (Eds.), *Deviance in international relations* (pp. 83–104). Springer.

Yangyue, L. (2014). *Competitive political regime and internet control: Case studies of Malaysia, Thailand and Indonesia*. Cambridge Scholars Publishing.

Yesil, B., Kerem Sözeri, E., & Khazraee, E. (2017). *Turkey’s Internet policy after the coup attempt: The emergence of a distributed network of online suppression and surveillance*. Internet Policy Observatory. https://repository.upenn.edu/internetpolicyobservatory/22

Yom, S. L. (2014). Authoritarian Monarchies as an Epistemic Community Diffusion, Repression, and Survival During the Arab Spring. *Taiwan Journal of Democracy*, *10*(1), 43–62.

Yom, S. L., & Gause III, F. G. (2012). Resilient royals: How Arab monarchies hang on. *Journal of Democracy*, *23*(4), 74–88.

Zittrain, J. (2003). Internet Points of Control. *Boston College Law Review*, *44*(2), 653–688.

Zittrain, J. (2008). *The future of the internet—And how to stop it*. Yale University Press.

Zürn, M. (2018). *A theory of global governance: Authority, legitimacy, and contestation*. Oxford University Press.

Appendix 1. List of codes.

1. Title

2. Date

3. Actor making statement

- BRICS
- China
- CSTO
- Other countries
- Russia
- SCO
- UNGA
- UNGGE
- UNSC

4. Organization

- ASEAN
- BRICS
- CSTO
- NA
- SCO
- UN
- WIC

5. International organization or regional organization?

- Global context
- IO
- NA
- Regional context
- RO

6. Document type

a. Legal publication

- Agreement
- Code of Conduct
- Convention
- Declaration
- Resolution
- Resolution draft

b. Official publication

- Position Paper
- Report
- Strategy

c. Official statement

- Communique
- Interview
- Press Release
- Speech
- Statement

7. Person making statement

8. Strategy

a. Socialization strategy

- Capacity-building
- Confidence-building measures
- Exchange expertise, best practices, joint research
    - BRICS
    - CSTO/PROKSI
    - SCO/RATS
- Express consensus
- Harmonization national legislation/common legal framework
- Importance regional cooperation
    - BRICS
    - CSTO

    - SCO
- Increasing cooperation and dialogue (that it is being increased)
    - International cooperation
        - ICANN
        - ITU
        - OECD
        - OEWG
        - UN
        - UNGA
        - UNGGE Information Security
        - UNIGF
        - WEF
        - WSIS
    - Regional cooperation
        - ASEAN/ARF
        - APEC
        - BRICS
        - CSTO/PROKSI
        - ECO
        - G20
        - OSCE
        - SCO/RATS
- Joint actions, operations and events
    - BRICS
    - CSTO/PROKSI/Center for Cyber Incidents
    - SCO/RATS
- Naming and shaming
- Praise norm-conforming behavior
- Provide technical assistance and professional training
    - BRICS
    - CSTO/PROKSI//Information Technology Center/University League
    - SCO/RATS
- Reputation and status

b. Persuasion strategy

- Try to increase the effectiveness and credibility of arguments
    - Coherency outcomes
    - Efficiency and effectiveness outcomes
- Frame arguments in a certain way (security frames):
    - Crime (including cross-border crime, cybercrime, drug-trafficking)
    - Extremism
    - International peace, stability, and security
        - Cyber warfare
        - Traffic rules
    - National political, economic and social security, social order
    - Rule of law
    - Separatism
    - Surveillance
    - Terrorism
    - Uprisings, protest, social unrest, revolution
- Link norms to other norms:
    - Human rights
    - International declarations, code of conducts, reports
        - BRICS eThekwini Declaration
        - BRICS Fortaleza Declaration
        - BRICS Ufa Declaration
        - G8 Deauville Declaration
        - SCO Agreement on Cooperation in the Field of IS
        - SCO Code of Conduct for Information Security
        - SCO Dushanbe Declaration
        - SCO Tashkent Declaration
        - UNGGE consensus reports
        - WSIS 2003 Geneva Declaration of Principles & other outcomes
    - International law
        - International Covenant on Civil and Political Rights/Article 19
        - Other UNGA resolutions
        - Other UNSC resolutions

        - UN Charter
        - UNGA Resolution A/RES/60/45
        - UNGA Resolution A/RES/64/25
        - UNGA Resolution A/RES/64/211
        - UNGA Resolution A/RES/65/41
        - UNSC Resolution 1624
        - UNSC Resolution 2354
    - Non-interference
    - Sovereignty & cybersovereignty
    - Territorial integrity
- Link norms to principles
    - Common destiny
    - Countering hegemony
    - Development, digital divide, digital equality
    - Mutual support, trust, benefit
    - Stability
    - Stakeholders in respective roles and responsibilities/importance states
    - One country one vote/democratic global governance/equality/multilateralism

c. Combination

- International norm building
    - Importance UN/international cooperation and dialogue
        - ICANN
        - ITU
        - UNGA
        - UNGGE Cyber Crime
        - UNGGE Information Security
        - UNHRC
        - UNIGF
        - UNSC
        - WIC/Wuzhen Summit
        - WSIS

    - Importance universally accepted norms, rules, principles, and laws
- Sequencing
    - As BRICS coalition
    - As CSTO coalition
    - As SCO coalition

Appendix 2. Overview of countries in Lührmann et al.'s regime type categories (2018).

Note: some countries can be listed in multiple categories due to regime transitions between 2011 and 2018.

Complete dataset zero model

Liberal democracy	Austria, Australia, Belgium, Benin, Bhutan, Botswana, Canada, Switzerland, Chile, Costa Rica, Cabo Verde, Cyprus, Czechia, Germany, Denmark, Estonia, Spain, Finland, France, United Kingdom, Ghana, Greece, Ireland, Israel, Italy, Japan, Republic of Korea, Lithuania, Luxembourg, Latvia, Mauritius, Netherlands, Norway, New Zealand, Poland, Portugal, Sweden, Slovenia, Slovakia, Tunisia, Trinidad and Tobago, United States, Uruguay, South Africa
Electoral democracy	Albania, Argentina, Bosnia and Herzegovina, Bangladesh, Burkina Faso, Bulgaria, Benin, Bolivia, Brazil, Bhutan, Botswana, Côte d'Ivoire, Colombia, Dominican Republic, Ecuador, Fiji, Georgia, Ghana, Guatemala, Guinea-Bissau, Guyana, Croatia, Hungary, Indonesia, India, Jamaica, Kenya, Kyrgyzstan, Comoros, Lebanon, Sri Lanka, Liberia, Lesotho, Lithuania, Latvia, Libya, Moldova, Montenegro, Macedonia, Mali, Mongolia, Mauritius, Malawi, Mexico, Niger, Nigeria, Nepal, Panama, Peru, Philippines, Pakistan, Poland, Paraguay, Romania, Serbia, Solomon Islands, Slovakia, Sierra Leone, Senegal, Suriname, El Salvador, Togo, Thailand, Timor-Leste, Tunisia, Turkey, Tanzania, Ukraine, Kosovo, South Africa, Zambia
Electoral autocracy	Afghanistan, Armenia, Angola, Azerbaijan, Bangladesh, Burkina Faso, Burundi, Belarus, Congo, Central African Republic, Congo, Côte d'Ivoire, Cameroon, Djibouti, Algeria, Egypt, Ethiopia, Fiji, Gabon, Gambia, Guinea, Equatorial Guinea, Guinea-Bissau, Honduras, Haiti, Iraq, Iran, Kenya, Kyrgyzstan, Cambodia, Comoros, Kazakhstan, Sri Lanka, Montenegro, Madagascar,

	Macedonia, Mali, Myanmar, Mauritania, Malaysia, Mozambique, Nigeria, Nicaragua, Nepal, Papua New Guinea, Pakistan, Palestine, Serbia, Russian Federation, Rwanda, Sudan, Singapore, Syria, Chad, Togo, Thailand, Tajikistan, Turkmenistan, Tunisia, Turkey, Tanzania, Ukraine, Uganda, Venezuela, Vietnam, Kosovo, Yemen, Zambia, Zimbabwe
Closed autocracy	United Arab Emirates, Bahrain, China, Cuba, Egypt, Eritrea, Fiji, Guinea-Bissau, Hong Kong, Jordan, North Korea, Kuwait, Lao, Libya, Morocco, Madagascar, Oman, Palestine, Qatar, Saudi Arabia, Somalia, South Sudan, Syria, Thailand, Turkmenistan, Uzbekistan, Vietnam, Yemen

Government criticism content count model

Liberal democracy	Austria, Australia, Canada, Germany, Denmark, Spain, France, United Kingdom, Greece, Israel, Italy, Japan, South Korea, Mauritius, Poland, Trinidad and Tobago, United States
Electoral democracy	Argentina, Brazil, Colombia, Hungary, Indonesia, India, Jamaica, Mexico, Peru, Philippines, Pakistan, Thailand, Turkey
Electoral autocracy	Armenia, Bangladesh, Iraq, Kazakhstan, Malaysia, Pakistan, Russian Federation, Thailand, Turkey, Ukraine, Kosovo, Yemen
Closed autocracy	United Arab Emirates, China, Kuwait, Saudi Arabia, Thailand, Vietnam

National security content count model

Liberal democracy	Australia, Belgium Canada, Switzerland, Germany, Spain, France, United Kingdom, Israel, Italy, Japan, South Korea, Netherlands, Poland, United States
Electoral democracy	Argentina, Bulgaria, Brazil, Colombia, Hungary, Indonesia, India, Mexico, Peru, Turkey, Kosovo
Electoral autocracy	Azerbaijan, Bangladesh, Belarus, Djibouti, Kazakhstan, Macedonia, Malaysia, Pakistan, Russia, Singapore, Turkey, Ukraine
Closed autocracy	United Arab Emirates, China, Hong Kong, Saudi Arabia, Thailand, Vietnam

Appendix 3. Descriptive statistics.

	N	Mean	Sd	Min	Max
Regime type	1155	1.65	0.98	0	3
Log terrorist incidents	988	-0.72	4.81	-6.91	9.54
Control of corruption	1169	-0.15	1.01	-1.83	2.40
Civil society organization consultation	1155	0.84	1.25	-2.31	3.85
Filtering capacity	1155	0.29	1.20	-2.98	2.81
Social media monitoring	1155	-0.10	1.37	-3.86	2.60
Internet penetration	1153	43.36	29.09	0.00	98.00
Log economic growth	1137	8.54	1.49	5.37	11.59
Foreign direct investments	1132	5.11	12.78	-43.46	252.31
Log population size	1169	16.22	1.53	13.13	21.05

Appendix 4. R code for data management.

```
################################################################################
#####

### PACKAGES

################################################################################
#####

library(reshape2)

library(plyr)

library(gdata)

library(countrycode)

library(dplyr)

library(data.table)

library(readxl)

library(xlsx)

library(naniar)

library(varhandle)

library(haven)

library(tidyr)

library(lubridate)


################################################################################
#####

### PREPARE DATA FOR ASSESSMENT OF TRENDS

################################################################################
#####
```

```
# 1. Load dataset Google

googledatasem = read.csv("google-government-removal-requests.csv", stringsAsFactors =
FALSE)

##Selecting relevant variables

googledatasem <- select(googledatasem, "Period.Ending", "CLDR.Territory.Code",
"All.Requests..Number.of.Requests", "All.Requests..Items.Requested.To.Be.Removed")


##Rename labels

googledatasem <- plyr::rename(x = googledatasem, replace = c("Period.Ending" = "year",
"CLDR.Territory.Code" = "country_code", "All.Requests..Number.of.Requests" =
"request_google"))

##Remove Europol

googledatasem <- subset(googledatasem, country_code!="")

##Remove last semester of 2009 and first semester of 2018, and years not corresponding with
Twitter dataset

googledatasem <- subset(googledatasem, year!="2009-12-31")

googledatasem <- subset(googledatasem, year!="2010-06-30")

googledatasem <- subset(googledatasem, year!="2010-12-31")

googledatasem <- subset(googledatasem, year!="2018-06-30")

##Save semesters as dates for time series analysis

googledatasem$year <- as.Date(googledatasem$year)

##Rename labels

googledatasem <- plyr::rename(x = googledatasem, replace =
c("All.Requests..Items.Requested.To.Be.Removed" = "request_items"))

###Replace NAs by 0s

googledatasem[is.na(googledatasem)] <- 0
```

```
################################################################################
#####

### PREPARE DATA FOR ANALYSIS

################################################################################
#####

# 1. Load dataset Google

googledata = read.csv("google-government-removal-requests.csv", stringsAsFactors =
FALSE)

##Remove excess variables

googledata <- select(googledata, "Period.Ending", "CLDR.Territory.Code",
"All.Requests..Items.Requested.To.Be.Removed")

##Rename labels

googledata <- plyr::rename(x = googledata, replace = c("Period.Ending" = "year",
"CLDR.Territory.Code" = "country_code", "All.Requests..Items.Requested.To.Be.Removed"
= "request_total"))

##Remove Europol

googledata <- subset(googledata, country_code!="")

##Remove last semester of 2009 and first semester of 2018, and years not corresponding with
Twitter dataset

googledata <- subset(googledata, year!="2009-12-31")

googledata <- subset(googledata, year!="2010-06-30")

googledata <- subset(googledata, year!="2010-12-31")

googledata <- subset(googledata, year!="2018-06-30")

##Recode semesters into years

googledata$year[googledata$year == "2011-06-30"] <- "2011"
```

```
googledata$year[googledata$year == "2011-12-31"] <- "2011"
googledata$year[googledata$year == "2012-06-30"] <- "2012"
googledata$year[googledata$year == "2012-12-31"] <- "2012"
googledata$year[googledata$year == "2013-06-30"] <- "2013"
googledata$year[googledata$year == "2013-12-31"] <- "2013"
googledata$year[googledata$year == "2014-06-30"] <- "2014"
googledata$year[googledata$year == "2014-12-31"] <- "2014"
googledata$year[googledata$year == "2015-06-30"] <- "2015"
googledata$year[googledata$year == "2015-12-31"] <- "2015"
googledata$year[googledata$year == "2016-06-30"] <- "2016"
googledata$year[googledata$year == "2016-12-31"] <- "2016"
googledata$year[googledata$year == "2017-06-30"] <- "2017"
googledata$year[googledata$year == "2017-12-31"] <- "2017"
##Sum based on double year and country
googledata$request_total <- as.numeric(googledata$request_total)
googledata <- as.data.table(googledata)
googledata <- googledata[, lapply(.SD,sum), by = "year,country_code"]

##Save year as numeric
googledata$year <- as.numeric(googledata$year)

# 2. Load separate Google dataset on reasons for content removal
googledata2 = read.csv("google-government-detailed-removal-requests.csv", stringsAsFactors
= FALSE)
```

```
##Remove excess variables

googledata2 <- select(googledata2, "Period.Ending", "CLDR.Territory.Code", "Reason",
"Items.Requested.To.Be.Removed")

##Rename labels

googledata2 <- plyr::rename(x = googledata2, replace = c("Period.Ending" = "year",
"CLDR.Territory.Code" = "country_code", "Reason" = "request_reason",
"Items.Requested.To.Be.Removed" = "request_number"))

##Remove Europol

googledata2 <- subset(googledata2, country_code!="")

##Remove last semester of 2009, 2010 and first semester of 2018

googledata2 <- subset(googledata2, year!="2009-12-31")

googledata2 <- subset(googledata2, year!="2010-06-30")

googledata2 <- subset(googledata2, year!="2010-12-31")

googledata2 <- subset(googledata2, year!="2018-06-30")

##Recode semesters into years

googledata2$year[googledata2$year == "2011-06-30"] <- "2011"

googledata2$year[googledata2$year == "2011-12-31"] <- "2011"

googledata2$year[googledata2$year == "2012-06-30"] <- "2012"

googledata2$year[googledata2$year == "2012-12-31"] <- "2012"

googledata2$year[googledata2$year == "2013-06-30"] <- "2013"

googledata2$year[googledata2$year == "2013-12-31"] <- "2013"

googledata2$year[googledata2$year == "2014-06-30"] <- "2014"

googledata2$year[googledata2$year == "2014-12-31"] <- "2014"

googledata2$year[googledata2$year == "2015-06-30"] <- "2015"

googledata2$year[googledata2$year == "2015-12-31"] <- "2015"
```

```
googledata2$year[googledata2$year == "2016-06-30"] <- "2016"

googledata2$year[googledata2$year == "2016-12-31"] <- "2016"

googledata2$year[googledata2$year == "2017-06-30"] <- "2017"

googledata2$year[googledata2$year == "2017-12-31"] <- "2017"

##Sum based on year, country and reasons for request

googledata2$request_number <- as.numeric(googledata2$request_number)

googledata2$year <- as.numeric(googledata2$year)

googledata2 <- as.data.table(googledata2)

googledata2 <- googledata2[, lapply(.SD,sum), by = "year,country_code,request_reason"]

##Spreading data on request_reasons

googledata2 = spread(googledata2, "request_reason", "request_number")


# 3. Match observations with other datasets for explanatory and control variables

##V-Dem

vdemdata2 = readRDS("V-Dem-CY-Full+Others-v9.rds")

###Selecting relevant variables

vdemdata2 <- select(vdemdata2, country_text_id, year, v2x_regime, e_fh_status,  e_democ, e_autoc, e_p_polity, v2xnp_regcorr, v2x_corr, v2cscnsult, v2ellocpwr, v2smgovfilcap, v2smgovsmmon, v2smorgavgact)

###Recode e_fh_status from NF, PF and F to 0, 1 and 2 respectively

vdemdata2$e_fh_status[vdemdata2$e_fh_status == "NF"] <- "0"

vdemdata2$e_fh_status[vdemdata2$e_fh_status == "PF"] <- "1"

vdemdata2$e_fh_status[vdemdata2$e_fh_status == "F"] <- "2"

vdemdata2$e_fh_status <- as.numeric(vdemdata2$e_fh_status)

###Selecting years 2012 to 2017
```

```
vdemdata2 <- subset(vdemdata2, year>="2011" & year<="2017")

###Changing country codes from iso3c to iso2c

vdemdata2$country_text_id <- countrycode(vdemdata2$country_text_id, 'iso3c', 'iso2c',
custom_match = c("PSG" = "PS", "SML" = "XS","XKX" = "XK", "ZZB" = "EAZ"),
warn=TRUE)

####Rename countrycode label

vdemdata2 <- plyr::rename(x = vdemdata2, replace = c("country_text_id" = "country_code"))

###Sum based on double year and country

vdemdata2 <- as.data.table(vdemdata2)

vdemdata2 <- vdemdata2[, lapply(.SD,sum), by = "year,country_code"]

###Assign missings: -66, -77, -88

vdemdata2[vdemdata2 == -66] <- NA

vdemdata2[vdemdata2 == -77] <- NA

vdemdata2[vdemdata2 == -88] <- NA


##Global Terrorism Database, National Consortium for the Study of Terrorism and Responses
to Terrorism

terrordata2 <- read_excel('globalterrorismdb_0718dist.xlsx')

###Selecting relevant variables

terrordata2 <- select(terrordata2, iyear, country_txt, nkill)

###Selecting years 2012 to 2017

terrordata2 <- subset(terrordata2, iyear>="2011" & iyear<="2017")

###Count number of attacks

terrordata2[is.na(terrordata2)] <- 0

data.frame(table(terrordata2$iyear, terrordata2$country_txt))
```

```
terrorattack2 <- data.frame(table(terrordata2$iyear, terrordata2$country_txt))

terrorattack2$Var1 <- unfactor(terrorattack2$Var1)

###Rename labels

terrorattack2 <- plyr::rename(x = terrorattack2, replace = c("Var1" = "iyear", "Var2" =
"country_txt", "Freq" = "terror_attacks"))

###Sum based on number of kills per year per country, not sure about the na.rm here

terrordata2 <- as.data.table(terrordata2)

terrordata2 <- terrordata2[, lapply(.SD,sum), by = "iyear,country_txt"]

###Combine number of kills and number of attacks data

terrordata2 <- merge(terrordata2, terrorattack2, by = c("iyear", "country_txt"), all=TRUE)

###Change NAs to 0s in number of kills

terrordata2$nkill[is.na(terrordata2$nkill)] <- 0

###Changing country codes from country names to iso2c

terrordata2$country_txt <- countrycode(terrordata2$country_txt, 'country.name', 'iso2c',
custom_match = c("Kosovo" = "XK"), warn=TRUE)

####Rename labels

terrordata2 <- plyr::rename(x = terrordata2, replace = c("iyear" = "year", "country_txt" =
"country_code"))


##Worldwide Governance Indicators

wgidata2 = read_dta("wgidataset.dta")

###Selecting relevant variables

wgidata2 <- select(wgidata2, countryname, year, cce)

###Selecting years 2012 to 2017

wgidata2 <- subset(wgidata2, year>="2011" & year<="2017")
```

```
###Changing country codes from country names to iso2c

wgidata2$countryname <- countrycode(wgidata2$countryname, 'country.name','iso2c', custom_match = c("Kosovo" = "XK", "Netherlands Antilles (former)" = "AN", "Korea, Dem. Rep." = "KP", "Korea, Rep" = "KR"), warn=TRUE)

####Rename countrycode label

wgidata2 <- plyr::rename(x = wgidata2, replace = c("countryname" = "country_code"))


##World Development Indicators

wdidata2 = read.csv("WDIData.csv", stringsAsFactors = FALSE, check.names = FALSE)

###Melting and spreading data

wdidata2 = melt(data = wdidata2, id.vars = c("Country Name", "Country Code", "Indicator Name", "Indicator Code"))

wdidata2 <- select(wdidata2, "Country Name", "Indicator Code", "variable", "value")

wdidata2 = spread(wdidata2, "Indicator Code", "value")

###Selecting relevant variables

wdidata2 <- select(wdidata2, "Country Name", variable, IT.CEL.SETS.P2, NY.GDP.PCAP.KD, BX.KLT.DINV.WD.GD.ZS, IT.NET.USER.ZS, SP.POP.TOTL)

###Selecting years 2012 to 2017

wdidata2$variable <- unfactor(wdidata2$variable)

wdidata2 <- subset(wdidata2, variable>="2011" & variable<="2017")

####Renaming labels

wdidata2 <- plyr::rename(x = wdidata2, replace = c("Country Name" = "country_code", "variable" = "year"))

###Changing country codes from country names to iso2c

wdidata2$country_code <- countrycode(wdidata2$country_code, 'country.name','iso2c', custom_match = c("Kosovo" = "XK"), warn=TRUE)
```

```
#Remove regions, world, etc.

wdidata2 <- subset(wdidata2, country_code!="NA")


# 4. Combine all datasets: googledata2, vdemdata2, politydata2, fhdata2, coupdata2, terrordata2, wgidata2, wdidata2

googledata2 <- merge(googledata2, googledata, union("country_code", "year"), all=TRUE)

googledata2 <- merge(googledata2, vdemdata2, union("country_code", "year"), all=TRUE)

googledata2 <- merge(googledata2, terrordata2, union("country_code", "year"), all=TRUE)

googledata2 <- merge(googledata2, wgidata2, union("country_code", "year"), all=TRUE)

googledata2 <- merge(googledata2, wdidata2, union("country_code", "year"), all=TRUE)

##Selecting countries with more than 500,000 inhabitants (SP.POP.TOTL), remove nas

requestdataclean <- subset(googledata2, SP.POP.TOTL > 500000)

##Dropping variables irrelevant reasons for requests: Adult Content, Bullying/Harassment, Business Complaints, Drug Abuse, Electoral Law, Fraud, Geographical Dispute, Impersonation, Obscenity/Nudity, Other, Reason Unspecified, Regulated Goods and Services, Religious Offence, Suicide Promotion, Trademark

summary(requestdataclean)

requestdataclean <- gdata::remove.vars(data = requestdataclean, names = c("Adult Content", "Bullying/Harassment", "Business Complaints","Drug Abuse", "Electoral Law", "Fraud", "Geographical Dispute", "Impersonation", "Obscenity/Nudity", "Other", "Reason Unspecified", "Regulated Goods and Services", "Religious Offense", "Suicide Promotion", "Trademark"))

##Replacing NAs by 0s where meaningful: reasons for request

requestdataclean$"request_total"[is.na(requestdataclean$"request_total")] <- 0

requestdataclean$"Copyright"[is.na(requestdataclean$"Copyright")] <- 0

requestdataclean$"Defamation"[is.na(requestdataclean$"Defamation")] <- 0
```

```
requestdataclean$"Government Criticism"[is.na(requestdataclean$"Government Criticism")]
<- 0

requestdataclean$"Hate Speech"[is.na(requestdataclean$"Hate Speech")] <- 0

requestdataclean$"National Security"[is.na(requestdataclean$"National Security")] <- 0

requestdataclean$"Privacy and Security"[is.na(requestdataclean$"Privacy and Security")] <- 0

requestdataclean$"Violence"[is.na(requestdataclean$"Violence")] <- 0
```

Appendix 5. R code for analysis.

```
################################################################################
#####

### PACKAGES

################################################################################
#####

library(ggplot2)

library(xts)

library(gridExtra)

library(psych)

library(car)

library(pscl)

library(plm)

library(lmtest)

library(lme4)

library(MASS)

library(gamlss.mx)

library(gamlss)

library(pscl)

library(texreg)


################################################################################
#####

### TRENDS (googledatasem)
```

```
##############################################################################
#####

# detrending (APPENDIX 6)

timeseries2 <- ts(googledatasem$request_items, start=c(2011,6,30), end=c(2017,12,31),
frequency = 14)

plot(stl(timeseries2, s.window = "periodic"))

# country trends (FIGURE 3)

p1 <- ggplot(subset(requestdataclean, country_code == "CH"), aes(x = year, y =
request_total)) + geom_line() + labs(title = "China (closed autocracy)", x = "year", y=
"requests")

p2 <- ggplot(subset(requestdataclean, country_code == "BR"), aes(x = year, y =
request_total)) + geom_line() +  labs(title = "Brazil (electoral democracy)", x = "year", y=
"requests")

p3 <- ggplot(subset(requestdataclean, country_code == "FR"), aes(x = year, y =
request_total)) + geom_line() +  labs(title = "France (liberal democracy)", x = "year", y=
"requests")

p4 <- ggplot(subset(requestdataclean, country_code == "DE"), aes(x = year, y =
request_total)) + geom_line() + labs(title = "Germany (liberal democracy)", x = "year", y=
"requests")

p5 <- ggplot(subset(requestdataclean, country_code == "IN"), aes(x = year, y =
request_total)) + geom_line() + labs(title = "India (electoral democracy)", x = "year", y=
"requests")

p6 <- ggplot(subset(requestdataclean, country_code == "RU"), aes(x = year, y =
request_total)) + geom_line() + labs(title = "Russia (electoral autocracy)", x = "year", y=
"requests")

p7 <- ggplot(subset(requestdataclean, country_code == "TR"), aes(x = year, y =
request_total)) + geom_line() + labs(title = "Turkey (electoral - closed autocracy)", x =
"year", y= "requests")
```

```
p8 <- ggplot(subset(requestdataclean, country_code == "GB"), aes(x = year, y =
request_total)) + geom_line() + labs(title = "United Kingdom (liberal democracy)", x =
"year", y= "requests")

p9 <- ggplot(subset(requestdataclean, country_code == "US"), aes(x = year, y =
request_total)) + geom_line() + labs(title = "United States (liberal democracy)", x = "year",
y= "requests")

grid.arrange(p1, p2, p3, p4, p5, p6, p7, p8, p9)


################################################################################
#####

### DESCRIPTIVE STATISTICS (requestdataclean)

################################################################################
#####

## Descriptives (APPENDIX 3)

describe(requestdataclean)


################################################################################
#####

### ASSUMPTIONS AND TRANSFORMATIONS

################################################################################
#####

## outliers

ggplot(aes(x = year, y = request_total), data = requestdataclean) + geom_point()

## distribution variables

requestdataclean$terror_attacks <- as.numeric(requestdataclean$terror_attacks)

d1 <- density(requestdataclean$request_total, na.rm = TRUE)
```

```
plot(d1)

d2 <- density(requestdataclean$v2x_regime, na.rm = TRUE)

plot(d2)

d3 <- density(requestdataclean$e_fh_status, na.rm = TRUE)

plot(d3)

d4 <- density(requestdataclean$e_democ, na.rm = TRUE)

plot(d4)

d5 <- density(requestdataclean$e_autoc, na.rm = TRUE)

plot(d5)

d6 <- density(requestdataclean$e_p_polity, na.rm = TRUE)

plot(d6)

d7 <- density(requestdataclean$terror_attacks, na.rm = TRUE)

plot(d7)

d8 <- density(requestdataclean$nkill, na.rm = TRUE)

plot(d8)

d9 <- density(requestdataclean$cce, na.rm = TRUE)

plot(d9)

d10 <- density(requestdataclean$v2xnp_regcorr, na.rm = TRUE)

plot(d10)

d11 <- density(requestdataclean$v2x_corr, na.rm = TRUE)

plot(d11)

d12 <- density(requestdataclean$v2cscnsult, na.rm = TRUE)

plot(d12)

d13 <- density(requestdataclean$v2smgovfilcap, na.rm = TRUE)
```

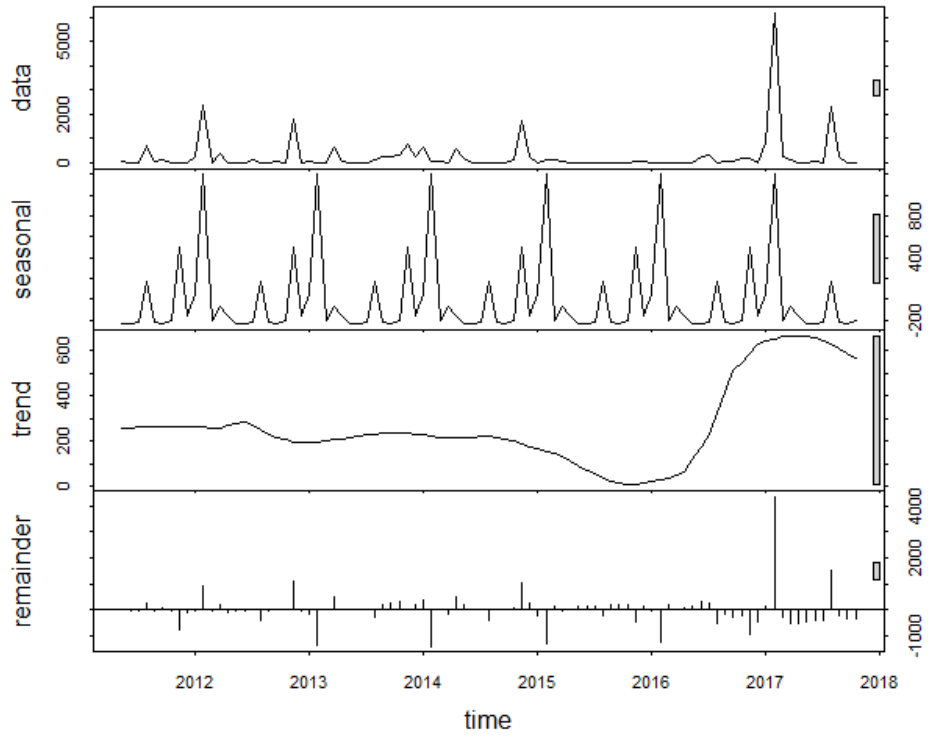
```
plot(d13)

d14 <- density(requestdataclean$v2smgovsmmon, na.rm = TRUE)

plot(d14)

d15 <- density(requestdataclean$IT.NET.USER.ZS, na.rm = TRUE)

plot(d15)

d16 <- density(requestdataclean$NY.GDP.PCAP.KD, na.rm = TRUE)

plot(d16)

d17 <- density(requestdataclean$BX.KLT.DINV.WD.GD.ZS, na.rm = TRUE)

plot(d17)

d18 <- density(requestdataclean$SP.POP.TOTL, na.rm = TRUE)

plot(d18)

## Log transformation: variable e_pt_coup, pcoup3, nkill, terror_attacks,
NY.GDP.PCAP.KD, BX.KLT.DINV.WD.GD.ZS, IC.REG.DURS, SP.POP.TOTL

requestdataclean$nkill[requestdataclean$nkill == 0] <- 0.001

requestdataclean$lognkill <- log(requestdataclean$nkill)

requestdataclean$terror_attacks[requestdataclean$terror_attacks == 0] <- 0.001

requestdataclean$logterror_attacks <- log(requestdataclean$terror_attacks)

requestdataclean$NY.GDP.PCAP.KD[requestdataclean$NY.GDP.PCAP.KD == 0] <- 0.001

requestdataclean$logNY.GDP.PCAP.KD <- log(requestdataclean$NY.GDP.PCAP.KD)

requestdataclean$SP.POP.TOTL[requestdataclean$SP.POP.TOTL == 0] <- 0.001

requestdataclean$logSP.POP.TOTL <- log(requestdataclean$SP.POP.TOTL)

## distribution dependent variable: zero inflated, so hurdle

ggplot(requestdataclean, aes(request_total)) + geom_histogram() + labs(x = "number of
requests", y= "frequency")

## distribution dependent variable: zero inflated, so hurdle
```

```
d1 <- density(requestdataclean$request_total, na.rm = TRUE)

plot(d1)

## multicollinearity

vif(glm(request_total ~ v2x_regime + logterror_attacks + cce + v2cscnsult + v2smgovfilcap +
v2smgovsmmon + IT.NET.USER.ZS + logNY.GDP.PCAP.KD +
BX.KLT.DINV.WD.GD.ZS + logSP.POP.TOTL, data = requestdataclean))


################################################################################
#####

### ANALYSIS (TABLE 7)

################################################################################
#####

requestdataclean <- plyr::rename(x = requestdataclean, replace = c("Government Criticism" =
"government_criticism", "National Security" = "national_security"))

##Government criticism

##Creating a dichotomous dependent variable for logistic part of hurdle model

requestdataclean$request_dummygc[requestdataclean$government_criticism == 0] <- 0

requestdataclean$request_dummygc[requestdataclean$government_criticism != 0] <- 1

subsetdatagc <- subset(requestdataclean, requestdataclean$government_criticism > 0)

##Binomial with logit link, year FE (i.e. BE)

logfegc1 <- glmer(request_dummygc ~ factor(v2x_regime, levels = c(3,2,1,0)) + (1 | year),
data = na.omit(requestdataclean), family = binomial(link="logit"))

logfegc3 <- glmer(request_dummygc ~ factor(v2x_regime, levels = c(3,2,1,0)) +
logterror_attacks + cce + v2cscnsult + v2smgovfilcap + v2smgovsmmon + IT.NET.USER.ZS
+ logNY.GDP.PCAP.KD + BX.KLT.DINV.WD.GD.ZS + logSP.POP.TOTL + (1 | year),
data = na.omit(requestdataclean), family = binomial(link="logit"))

summary(logfegc1)
```

```
summary(logfegc2)

exp(0.96)

##Between countries

nbgcfe1 <- gamlss(government_criticism ~ factor(v2x_regime, levels = c(3,2,1,0)) +
re(random = ~ 1 | year), data = na.omit(subsetdatagc), family = NBI)

nbgcfe2 <- gamlss(government_criticism ~ factor(v2x_regime, levels = c(3,2,1,0)) +
logterror_attacks + cce + v2cscnsult + v2smgovfilcap + v2smgovsmmon + IT.NET.USER.ZS
+ logNY.GDP.PCAP.KD + BX.KLT.DINV.WD.GD.ZS + logSP.POP.TOTL + re(random =
~ 1 | year), data = na.omit(subsetdatagc), family = NBI)

summary(nbgcfe1)

summary(nbgcfe2)

exp(3.27)

exp(5.02)

htmlreg(list(logfegc1, logfegc2, nbgcfe1, nbgcfe2), file = "hurdlegctotal.doc", inline.css =
FALSE, doctype = TRUE, html.tag = TRUE, head.tag = TRUE, body.tag = TRUE)

##National security

##Creating a dichotomous dependent variable for logistic part of hurdle model

requestdataclean$request_dummyns[requestdataclean$national_security == 0] <- 0

requestdataclean$request_dummyns[requestdataclean$national_security != 0] <- 1

subsetdatans <- subset(requestdataclean, requestdataclean$national_security > 0)

##Binomial with logit link, year FE (i.e. BE)

logfens1 <- glmer(request_dummyns ~ factor(v2x_regime, levels = c(3,2,1,0)) + (1 | year),
data = na.omit(requestdataclean), family = binomial(link="logit"))

logfens2 <- glmer(request_dummyns ~ factor(v2x_regime, levels = c(3,2,1,0)) +
logterror_attacks + cce + v2cscnsult + v2smgovfilcap + v2smgovsmmon + IT.NET.USER.ZS
+ logNY.GDP.PCAP.KD + BX.KLT.DINV.WD.GD.ZS + logSP.POP.TOTL + (1 | year),
data = na.omit(requestdataclean), family = binomial(link="logit"))
```

```
summary(logfens1)

summary(logfens2)

exp(1.68)

##Between countries

nbnsfe1 <- gamlss(national_security ~ factor(v2x_regime, levels = c(3,2,1,0)) + re(random = ~ 1 | year), data = na.omit(subsetdatans), family = NBI)

nbnsfe2 <- gamlss(national_security ~ factor(v2x_regime,  levels = c(3,2,1,0)) + logterror_attacks + cce + v2cscnsult + v2smgovfilcap + v2smgovsmmon + IT.NET.USER.ZS + logNY.GDP.PCAP.KD + BX.KLT.DINV.WD.GD.ZS + logSP.POP.TOTL + re(random = ~ 1 | year), data = na.omit(subsetdatans), family = NBI)

summary(nbnsfe1)

summary(nbnsfe2)

exp(-3.49)

htmlreg(list(logfens1, logfens2, nbnsfe1, nbnsfe2), file = "hurdlenstotal.doc",  inline.css = FALSE, doctype = TRUE, html.tag = TRUE, head.tag = TRUE, body.tag = TRUE)

htmlreg(list(logfens1, logfens2, nbnsfe1, nbnsfe2, logfegc1, logfegc2, nbgcfe1, nbgcfe2), file = "hurdlensgctotal.doc", inline.css = FALSE, doctype = TRUE, html.tag = TRUE, head.tag = TRUE, body.tag = TRUE)
```

Appendix 6. Decomposition of the number of items requested to be removed to Google between 2011 and 2018.



Appendix 7. List of publications.

Flonk, D. (2021). Emerging illiberal norms: Russia and China as promoters of internet content control. *International Affairs, 97*(6), 1925-1944.

Flonk, D. (2021). Book Review: The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. *Convergence: The International Journal of Research into New Media Technologies, 27*(1), 283-288.

Flonk, D., Jachtenfuchs, M., & Obendiek, A. S. (2020). Authority conflicts in internet governance: Liberals vs. sovereigntists?. *Global Constitutionalism, 9*(2), 364-386.