One Internet to Rule Them All

Ezekiel Rochmis, MAIR '23

Abstract

As the internet has become increasingly pervasive worldwide, autocratic regimes have taken measures to restrict their citizens' access to the web. Interestingly, these crackdowns have been predominantly conducted unilaterally by states, despite the internet being a global platform with shared content. This raises questions as to why states would opt for independent content moderation rather than engaging in multilateral digital governance. Drawing on shared burden and state sovereignty literature, particularly digital state sovereignty, this paper argues that states should be more willing to participate in multilateral digital governance to protect their economic interests and sovereignty. The study outlines a novel approach to evaluate two conditions that influence states' engagement in multilateral governance regarding the internet. Firstly, states experiencing higher levels of cyber incidents are expected to be more inclined to participate in multilateral efforts to enhance incident responses. Secondly, the degree of openness in a state's society and internet usage is considered, as both democracies and autocracies have exhibited reluctance to engage in multilateral governance, while mixed regimes tend to demonstrate greater openness. This paper presents a potential framework for conducting such a study and highlights possible limitations associated with the choice of methods.

Through a network of cables that span the globe, we have achieved the deepest connections between citizens of the world and it's all thanks to the internet. A series of interchanges, satellites, cables, and servers brings nearly every corner of the world into conversation with each other. The internet is the most transformative development in human communications, allowing the near simultaneous and instantaneous transmission of anything to everyone. Yet with the internet becoming a mainstay in modern society we have seen a rise in the number of states who look to impose controls on the citizens' access to the open web. States like Iran and Russia have passed laws that forbid posting or accessing certain content, while China has developed a complex network of censorship mechanisms to prevent access to content considered subversive by the state. The freedom the internet provides to citizens around the world is an unprecedented occurrence. This ability of citizens to engage in anonymous dissent and political discussions is a threat to the powers of autocracies, as prior to the internet self-censorship and laws prevent widespread dissemination of ideas. Following the Arab Spring of 2011 the world watched with bated attention as the power of organizing protests via social media threatened significant changes to Arab autocracies and potentially others in the future. Autocracies took swift note of this power and at once sought ways to prevent a similar occurrence happening in their state.

What is confounding is that all these autocracies unilaterally create censorship regimes and implement restriction of information laws. For example, China should prefer that both their citizens domestically and abroad should be unable to see images of “Xi-Jing Pooh” (image 1). But unilaterally they are unable to do more than ban its spread and use on the Chinese censored internet. Even then, Chinese citizens have taken it upon themselves to keep it in their meme culture through code phrases and the use of virtual private networks to spoof their locations. At

the same time this direct censorship of the internet has given rise to many Chinese competitors to US based social media, and other digital platforms. This parallel set of applications has created a massive domestic economy for China and has even allowed them to try to sell other states on these platforms as alternatives to western services. But if China used a multilateral approach, they would be able to avoid this circumnavigation of censorship by simply having the image scrubbed in its entirety from the internet and have potentially saved millions on research and development costs of their censorship regime.

Multilateral governance of the internet is a new concept, as much of the internet's lifespan has existed under the US's "wild west" framework where no single state could control what is posted. Yet in the mid 2000's the United Nations convened a Group of Governmental Experts (GGE) to discuss "developments in the field of information and telecommunications in the context of international security". As of May 7, 2023, this GGE had been wrapped into a United Nations General Assembly Open Ended Working Group session dedicated to the application of UN norms and standards to the Internet. These two sessions mostly focused on individuals' rights to internet access and safety rather than on the concerns of the state. State's concerns were instead heard within the International Telecommunications Union (ITU), but any movement on putting international regulations in place was swiftly blocked by the United States.

This is essentially where the conversation on multilateral digital governance ended, but if we broaden the scope, we see states work together to combat cybercrime through similar mechanisms. This approach is the closest thing we have to true multilateral governance, and we see it at scale as wealthier states must partner with poorer states to apprehend cybercriminals. This leaves one last potential pathway; a mix of unilateral and multilateral agreements. Sounds impossible right, what state would be crazy enough to give up part of their sovereignty to other

states then spend the money and time to regulate their own internet. The closest example we have is the EU and their cybercrime laws. Within the borders of the EU countries, individuals are not allowed to post or view pornographic content that involves under aged individuals or deep fakes of real people. This gives powers to the state to enforce their own sovereign beliefs on the internet while protecting their citizens. But this measure only affects those within the EU. Deep Fake porn still is accessible in other countries and will be created there and without constant monitoring the EU is unable to prevent the spread of this content. However, states within the EU have been able to stop their production and some procurement within their borders, which is the first step to larger regulations.

The areas of pornographic content and hate on the internet are viewed by most rational individuals to be a social good. But what happens if the EU decides instead to ban the use of Twitter or Facebook within state borders? This movement toward digital global governance (DGG) can be seen as a social good in some ways, but if taken too far it may serve to strip individuals of their right to freedom from harm. This is why understanding how the world is progressing to DGG is important, because it can both do great good for our society but could also cause the greatest social crackdown ever.

Understanding these three ways of digital governance, why then do states take unilateral action when it comes to digital governance, rather than use IOs? The introduction and resolution of global governance issues is one of the specialties of IOs and as such, we should expect to see the same when it comes to digital governance since it is quite like that of the International order.

Lit Review

The internet has been one of the most powerful forces in the last century but what makes it so interesting is its inherent interconnectedness, both through the way it connects us digitally

and physically. Yet not every state sees the internet equally, some view it as an existential threat to their power, whereas others see it as a tool to shape a fairer society. But how can you rectify these two distinct desires, one for a globally connected platform that frees people and one that the state has complete control over. This is the struggle that lies at the heart of digital global governance (DGG), "the norms, institutions, and standards that shape regulation around the development and use of [the] technologies" of the internet (Runde & Sundar 2021).

Understanding that DGG is a continuous discussion between states on what form the internet takes, we should expect to see International Organizations play a larger role in this discussion given the fact that the internet is a keystone in the modern global economy. Yet all the discussions on how to regulate the internet have fallen to the wayside in favor of digital sovereignty, the idea that each state should be able to dictate the who, what, where, and how of the internet and access to it within their borders. To understand more about this conflict between DGG and digital sovereignty we turn to the literature on international economic cooperation, sovereignty, internet fragmentation, DGG, and human rights.

Economic Cooperation

The core idea behind this question is that the internet is a critical sector to the modern global economy and as such should be regulated similarly to other materials that are regulated and discussed. More exactly, we should expect to see it regulated similarly to telecommunications, like that of the ITU. The ITU has been at the forefront of discussion concerning the internet yet when they attempted to discuss the internet, states like the US blocked them from discussing critical aspects related to the internet's openness (Larionova and Shelepov 2021). Within these spaces the internet is held as a key tool in the modern global economy and as such most parties are afraid of what regulation would look like. No one is

willing to touch the economic aspects of the internet, intellectual or material (Sukhodolov, Popkov and Kuzlaeva 2017), because these portions of the internet are the same that everyone uses. This ties back directly into a more general desire for governance over the internet. As a side note one explanation that is yet to be explored is the idea of legitimacy within these IOs (Dellmuth 2019). However, DGG legitimacy among citizens matters little versus that of the view of DGG legitimacy among states. This idea of IO legitimacy is interesting and yet to be explored fully and is one potential explanation for what we see currently.

DGG, Fragmentation, and Sovereignty

The term DGG may be new, but discussions on the governance of the internet are not new and date all the way back to the birth of the world wide web. One of the more important early papers is Daniel Drezner's 2004 paper on bringing states back into the governance discussion. With a focus on how globalization affects the discussion on the internet on IOs, Drezner fears that the internet weakens the state's role in global governance. However, 20 years later the fact that states have more power over their own internet than ever has proven these fears to be a relic of the dot com boom. We have not seen states lose any amount of governance power because of the internet; in fact, we have seen a new realm of global governance born. In a recent 2022 paper by Jia and Chen they argue that DGG is a new concept and is a response to the "techlash" of the 2020's. I find this idea that DGG new to be incorrect given Drezner's identification of other DGG like processes carried out in the late 1990's and early 2000's. DGG is not a new idea and is innately tied into globalization and is at threat from internet fragmentation.

Internet fragmentation is the division of a unified internet into regionalities based on level of access. Think Russia's RUnet or China's great firewall, a security system that filters what

Chinese citizens can access, where what the citizens are allowed to see, and posts are regulated by the government and that outside users cannot see in. Fragmentation is the result of the ad hoc nature of the current DGG regime, where no states can agree on a common set of principles and norms and instead forge their own path. This division threatens DGG by shifting internet norms and regulations to a state level, while causing platform integration issues along with loss of economic functions by simply removing certain players from being able to participate in certain areas of the web. This process has come about due to two concepts: The internet is inherently a democratizing force, and states wish to preserve their digital sovereignty.

One of the earliest discussions on the internet as a democratizing force frames the idea around civic culture. The idea that the society in which the citizens live dictate the sort of governmental structures around them and the ways in which they interact with formal political systems. It is argued that media, specifically media hosted on the internet, has the power to both empower and disempower citizens (Dahlgren 2000). This discussion on civic culture is why many states push back against the idea of DGG as the current form of the internet is very western and incredibly open which is viewed as a threat to state security, with the best example of this occurring is in Russia. The Russian people were early mass adopters of the internet and became highly online people. However, following the Arab Spring of 2011, the Russian state government began to implement more restrictions on the people's access to content and began more heavily censoring posts, out of fear that their citizens would use these platforms to protest their government. They used their position as the primary internet provider to restrict websites, launch mass internet-media propaganda, and censor opposition. Russia still maintains that the way they have developed the RUnet is a model for other countries as it protects the digital sovereignty of the states and represents an alternative to the western model.

Digital sovereignty is an offshoot of sovereignty but as it applies to the internet and internet infrastructure. In recent years scholars have questioned whether digital sovereignty is an even real concept given that no one state is able to control the platforms (Mueller 2019). Conversely, states are the primary point of access for the internet as they control and service the physical infrastructure that is required for the internet. When these questions were brought forward inevitably China and Russia pushed out their chest and claimed that any norm and regulation setting that they do not agree on violates their digital sovereignty. But even with this push back to western norm setting we should still expect these countries to agree on setting norms and regulations in areas in which preferences overlap.

DGG, fragmentation, and digital sovereignty are the central focus of this paper, but we also must explore the efforts being undertaken in DGG now.

Multilateralism in Technology

Given that this paper focuses on how states engage in multilateral governance over the internet it is important to understand how this multilateralism currently functions. As discussed earlier, the current pathways through the GGE and UNGAOWEG are representative of states applying their experts to the problem. However, this paints a small picture of what is currently happening.

Before we talk about multilateralism on the internet it is important to understand standards setting organizations and the role they play. The ITU is an international regulatory body that brings together members of the international community to deliberate and decide on best practices and standards for telecommunication devices. These standards are especially important as they dictate which technologies must be used and how they can be used. This form of multilateralism is the most aspirational for regulation of the internet but attempts to have the

ITU set standards have been blocked by the US and their allies (Kaska et al 2019; Tekir 2022), due to fears of Chinese influence and desires within this body.

Moving from a general discussion we can now discuss how states currently engage in multilateralism on the internet, combating cybercrime. Cybercrime is a broad category of criminal activities that utilize the internet for illegal activities. These agreements are often designed and deployed on a case-by-case basis to capture specific criminals. However, there are more long-standing missions through IOs such as Interpol that give specific powers and resources to reduce a type of criminal activity. This current regime of multilateral agreements is important to understand but they are geopolitical issues and not around the internet.

Human Rights, how they apply to the internet.

Out of all the topics covered in this lit review, human rights may seem like a far cry. Yet the only IO acting on digital global governance is the UN with a focus on how the Declaration on Human Rights applies to the internet. As it stands article 19 of the United Nations Human Rights Council now includes the "promotion, protection and enjoyment of human rights on the Internet", this paired with the United Nations General Assembly Open-Ended Working Group (UNGA OEWG), formally the Group of Governmental Experts (GGE), is focused on determining how human rights and the UN charter apply to the internet. The current working understanding is that both elements apply to the internet and as such states should follow them. Yet many states do not buy into these concepts and still maintain that they will operate however they want under digital sovereignty. Outside of policy the discussion on how technologies can be used to suppress or promote human rights has become a burgeoning field. Dragu and Lupu 2021 and Lee 2022 look like the ways in which these technologies alter socio-political structures. These papers both contradict each other's claims about the effect of technology on levels of

autocracies, but both do stress the need to understand the intersection of human rights and technologies. Which leads to one of the largest questions on the internet: Is there a need for an internet declaration of human rights?

The general outcome from this research will be new insights into the way states interact with governance within the digital sphere. This should aid in building on why states take the actions they do and what they really want from the internet. While at the same time trying to understand how the global internet will look in the future.

Within this question we have two agents operating: States and IOs. In the case of the question our primary actors are States, their involvement, and choices surrounding DGG, and DG whereas their interaction within, and with IOs is our primary interest. To better understand these relationships, I propose two hypotheses.

Hypothesis 1: States that experience more frequent cybersecurity incidents are more likely to engage in multilateral DG.

This hypothesis seeks to answer a simple question about state capabilities and if that affects the choice to engage in DG. Through the understanding of the logic of the dog that did bark (Lupovici 2021), we should expect states that report higher frequencies of cyber incidents to look to a multilateral approach due to lack of internal capabilities at deterring and solving these attacks, and instead hoping to gain stronger capabilities or use norm setting to clean up their systems. However, stronger states should be avoiding these partnerships due to free riding and the lack of altruism. I contest that stronger states have an incentive to partner with weaker states to curtail cybercrime and prevent mass malware executions. I.e., this is burdening sharing, where the stronger states may not be willing to sacrifice their own security and technologies to help

weaker states improve theirs. I believe weak states will attempt to form multilateral DG, whereas strong states will not. In the case of WannaCry, the launch point for this malware was vulnerable systems within Southeast Asia. This malware then began to spread through the systems of the banking hubs within Singapore and to the rest of the windows devices around the world. Only through collective action of state cyber incident response teams was a vulnerability in the malware identified and exploited. It is in the best interest of states to avoid having critical internet-connected systems to collapse as it threatens the stability of the world economy.

Hypothesis 2: States that are more oppressive and states that are less oppressive are less likely to engage in multilateral DG.

This hypothesis is built on the logic that any given state values their sovereignty in the digital realm. Specifically, it targets the idea that those who avoid, or place restrictions will avoid hand-tying and other aspects that would radically transform their internet platforms. This is simply since the internet as a tool can serve both to empower or disempower the citizens based on regulations and norms (Dahlgren 2000; Adams and Albakajai 2016). States want to avoid having to fall in line with regulations of other states if they believe it to be against their best interests. At the same time due to the globalized nature of the internet, without extensive webpage blocking and censorship, it is impossible to exert any real amount of sovereignty over your own internet (Mueller 2019). Even in China they are dealing with this, as citizens can get their firsthand virtual private networks that let them break out of the Chinese Internet via location spoofing. With these threats to the regimes internet controls China would want to logically avoid being forced into applying western decisions to their internet. Similarly, more politically free states wish to maintain complete internet openness due to the ways in which it

democratizes information and media. As we have seen, the internet has become a powerful tool for grass-roots political movements to attract and inform their members. Any amount of regulation could cause these groups to fold and weaken the democratic process. This leaves mixed regimes as states who are more likely to want to engage in multilateral DG. They have a desire to grant their citizens access to the web due to economic and social benefits, but at the same time desire a more structured environment than the western internet version provides. Singapore is one such example where they enjoy the economic benefits provided by an open web but perform limited censorship and control to avoid dissent groups forming.

To note the expected outcome from this relationship is curvilinear, with most states seeking to engage in multilateralism being those of mixed regimes rather than true democracies or autocracies.

However, these hypotheses do not cover the entire scope of this question due to how broad the topic really is. What is missing from the literature review is a question related to human rights on the internet, as this paper is not focused on the application or question of human rights to the internet and is instead interested in how states think about norms of globalized institutions.

Methods

To evaluate both hypotheses 1 and 2, I need to collect and modify data on cyber incidents, levels of democracy, internet openness, and engagement in multilateral digital governance. To start, I found pre-existing databases that cover much of what I am interested in.

Pre-existing Databases

Council Foreign Relations (CFR) Cyber Operations Tracker Database

One of the most important databases that collects data on the number of cyber incidents is the CFR cyber operations database. It is an open-source database that catalogs all officially known state-sponsored cyber activity since 2005, and only includes "data in which the perpetrator, also known as the threat actor, is suspected to be affiliated with a nation-state." This dataset was chosen over the similar Verizon's Vocabulary for Event Recording and Incident Sharing (VERIS) framework. VERIS also offers "an open and free repository of publicly reported security incidents in VERIS format," that collects self-submitted data on incidents using the VERIS framework. Between the two datasets there is an overlap, however the VERIS database is much more extensive as it covers more business level attacks, whereas CFR collects data more relevant to civil society and states. Due to the nature of these databases, I had initially considered using both to provide a strong insight into cyber incidents. However, there is an overlap between both and due to the separate ways in which certain events were coded differently makes it difficult to identify repeated incidents. To avoid potential issues arising from this conflict I have chosen to only use the CFR database as it is more relevant to the domain in which this paper is interested, however VERIS is still viable to be used in this research.

CFRs database provides 770 observations dating back to 2005. To operationalize this data for this study we care about two categories: date and victim. Date is in standard formatting which makes it easier to work with whereas victim has a non-standard format with each of the 770 observations being a comprehensive naming of the victim, and event. To work CFR's data each of the 770 observations will be normalized to be named after the country in which it occurred only. In the end, the only data we care about taking from this database is the number of incidents so the coding within my data would be the number of incidents or a N/A for no occurrence. The choice to use N/A rather than a zero code comes from the real world, where these countries or

their business' may not be reporting incidents and it would be incorrect to code them as zero. This does however lead to their exclusion in the conclusion of the hypothesis. To achieve the best results this set of data would be run twice, once with N/A values being held as N/A and a second time where they are simply held as zero. This allows us to evaluate if there is a change in significance when these observations are added to the dataset.

Freedom House

The other major databases which I will be using are the Freedom House democracy and internet freedom indexes. These databases provide a comprehensive breakdown of a state's level of democracy and internet freedom on numerous dimensions. These databases provide information for both hypotheses as it also attaches a government type to each state-observation. The values captured allow for a granular study of certain aspects of democracy and internet freedoms, however it is most likely that the only thing that would matter is the overall score of democracy and internet freedom. The largest drawback of these datasets is that although the freedom house has data dating back before 2005 their internet freedom public data starts in 2011 and ends in 2022, making this the limiting factor in data collection.

Data to be collected.

Even with all the pre-existing databases out there, there does not exist a single collection of multilateral agreements as it relates to the internet and cyber security. This means to be able to fully evaluate these hypotheses I need to collect data on these agreements. For example, by cataloging each state who signed onto the UNGA Open ended working group (OEWG), and the two UN groups of governmental experts that focused on the internet. Further, it is important to consider cyber-crime agreements, through places like Interpol, or multilateral information sharing schemes to fall into this broader category of multilateral digital governance. This data

collection needs to be attempted at least once before changes could be made in what information is both available and relevant.

Final dataset

The first step is to create a simple database that catalogs each state's signature or participation in a multilateral DG agreement. I would code it as not applicable for states who potentially could not sign onto the agreement, zero for members who could sign but did not sign onto the agreement, and one for signing onto the agreement. To note I choose not to weigh participation/non-participation in different agreements as it is difficult to make judgment calls on the values of multilateral agreements in a vacuum. Further, there is a compelling case for weighing certain participations but because of the difficulty in tracking progress in implementation I find it best to normalize each participation. This does mean that the conclusions that I draw are not definitive and that potentially these states are more interested in DGG rather than a solid idea that they are interested in DGG. However, if this study could run continuously, weighing agreements is particularly important to track DGG participation as the type of agreement becomes more important than the number of agreements.

Year	Country	Number of Cyber Incidents	Freedom House Freedom Score	Freedom House Internet Freedom Score	Total Number of agreements	UNGA sign	Some multi-agreement
2015	United States	Some Number	1	1	Some Number 2	1	1

2016	United States	Some other number	2	1	Some other number 2	1	0

Above is a simplified version of the dataset that would be created for the paper. The largest missing category is the freedom house data. It would continue further to the right, with a deeper break in which dimensions they scored. One of the potential pitfalls within this data collection framework is the near infinite number of cyber-related multilateral agreements and how they directly affect the data. To get around this, I have included a variable for the total number of agreements signed. This does affect model creation for this paper.

Potential Models

My first consideration for this paper was to run a model for each multilateral agreement, and because it is a binary sign or no sign, I had planned to use a logit. However, as stated above this yields an unwieldy amount of work to approach a conclusion. Due to this issue, instead testing on the number signed becomes much more reasonable. Therefore, I have decided to use Poisson or negative binomial regression, depending on how dispersion of the data looks at the end of the data collection process. This allows for the inclusion of both binary variables (yes or no to signing agreements) and total count of how many agreements states signed. When it comes to how to model this interaction, we would potentially be using a generalized linear model using the Poisson distribution with our primary interest variable being the total number of agreements as it relates to all the other variables of interest.

Sources of Error

As stated in the prior sections, this paper is rife with potential data errors. Most of these potential errors come from the ways in which I have chosen to code the data. The largest potential issue arises from the way in which I code agreement signatures. I feel that a data collection process that ignores smaller agreements fails to understand how potential DGG could play out, however this leads to many observations of states being n/a's which invalidates the inclusion of them in a test. I attempt to account for this using a total count variable rather than including each multilateral DG observation. However, this then introduces an issue that most states will have a similar count of observation that is small. I cannot build a way to account for this until I have completed the data collection process, but it should be known that this is potentially an incorrect way to collect data on multilateral agreement signings.

Along similar lines, the data for cyber incidents will have the exact same issue as multilateral signing. The fact is that most states will be recorded as n/a simply due to the lack of reporting on occurrences by the state. This does not account for the possibility that a state did have any occurrences of cyber incidents because it looks the same as no report. To really conduct this study more work needs to be done to cross-check numerous sources of reporting. In this case I would argue that a crossing of the VERIS database and CFR COTD would be a good start, but then accounting for other sources such as Thales or other telecommunication databases would provide the most accurate data possible.

In the end I believe in the need for a data-driven study of these questions, but it may be more feasible to start with a normative discussion and case studies.

Within the international community there are large scale agreements used to regulate certain industries or technologies, not all states sign on but enough follow them to make the regulations work. The same cannot be said for the internet as of today; it is still relatively young technology

and thus there are fewer internationally recognized agreements surrounding it. To be able to study why states have yet to make these moves towards regulation of the internet and as to how effective the current set of DGG is we must start by laying out a few assumptions.

The most important assumption we can make is that states inherently desire to have the maximum level of sovereignty, be it territorial or digital (Glen 2014). Yet, states are more than willing to give up parts of their sovereignty to engage in a structured international order to further some set of goals. In the case of DGG it is assumed that states will be willing to sacrifice sovereignty in the digital space because it is an economic platform, and an economic driver (Sukhodolov, Popkov and Kuzlaeva 2017; Larionova, Marina, and Andrei Shelepov 2021). They also should be more willing as most regulations seek to reduce digital harm and bridge the digital divide thus making the platform more internationalized, growing the reach of certain economies.

Another core assumption we must make is that states will not solely go unilaterally or multilaterally into DG but take on a mixture of both (Jia and Chen 2022). With this assumption it places an emphasis on there being a scale of engagement within DGG with one end being entirely unilateral and the other being entirely multilateral. For example, the US National Institute of Standards and Technology, in their cybersecurity 2.0 framework expresses the need for deeper engagement with Standards Developing Organizations (SDOs, also known as Standards Setting Organizations SSOs) for a more standards-based approach to cybersecurity and privacy. Following similar logic, states multilateral engagement will not take the same form across partners and time, as shifts in needs and geopolitics prevent a core multilateral approach from forming. This is seen in China dropping their crack down on fentanyl with the United States over the trade war launched by president trump. These policing agreements are the backbone of cyber-crime agreements as police take the most direct engagement in the domain of

cyber regulation. However, they want these deeper engagements to occur as a product of US cyber norms and functions.

The last yet perhaps most prudent idea is that due to the nature of the internet and global order it may simply be impossible to regulate the body through something like the ITC or UN and instead regional organizations or special interest IOs may be the real home. Even then there is still a lack of real effort to shape the norms and enshrine the rights of those who use the internet into law. Within bodies like the EU, they have put in place content censorship of potentially harmful content such as deepfake and child pornography. Yet rather than enshrine these norms, they are regulated under policing efforts of cybercrime divisions of each country's police. These norms are like that of western norms in institutions and yet have been regulated to being crime stopping provisions. Outside of this there have been discussions on applying things like the Declaration of Human Rights and the laws of armed conflict to cyberspace (Xinmin 2016). If states chose not to regulate it, some believe it should be treated like the international order and simply be balkanized into different spheres (Lambach 2019).

Conclusion

As this paper does not conduct a complete study it is disingenuous to draw conclusions about the state of the world. However, this paper sets up a potential study that would prove foundational in understanding how states engage multilaterally when it comes to the internet. Understanding if the concept of shared burden is driving states to work together on cyber-crime is particularly important given that most cyber-crimes perpetrators live outside the state in which it is conducted, and as these attacks become more complex and large-scale, everyone is potentially a target. Furthermore, understanding which type of government wants to engage in multilateral DG represents a huge step forward in understanding the internet. Currently it is

assumed that autocratic and mixed regimes are happy with the current state of the internet as most of their citizens do not have the means or the time to find ways to avoid censorship, while democracies push for changes to the internet to better reflect the values of the international community.

One form of multilateralism that this paper chooses not to cover is the sale of parallel platforms, and censorship technologies. China's goal of separating itself from the global web has resulted in the creation of parallel sets of platforms, and deeply complex censorship technologies. China has expressed on more than one occasion an openness to helping other states set up similar systems. States like the UAE and Iran have decided that creating an Islamic internet is a priority for them as they fear giving their citizens access to the web will result in another Arab Spring. The sale of these technologies is another pathway in understanding how states work at the international level to shape the internet to their desires. This discussion may not seem important now, but as the internet begins to pervade increasingly into the daily life of everyone around the world, how people are able to access and use the internet becomes paramount.

Appendix

Image 1. A famous photo of US President Barack Obama and Chinese President Xi Jing Ping walking together. Chinese netizens likened Xi to Winnie the Pooh and began to meme him. The Chinese censorship regime quickly banned the image above along with images of Winnie the Pooh and any reference to the characters from the stories.

10. Why Does Xi Jinping Fear Winnie the Pooh? 2018. Times Of India Times Of India. https://static.toiimg.com/thumb/msid-65311451,width-1070,height-580,imgsize-769328,resizemode-75,overlay-toi_sw,pt-32,y_pad-40/photo.jpg (May 10, 2023).

Figure 1.

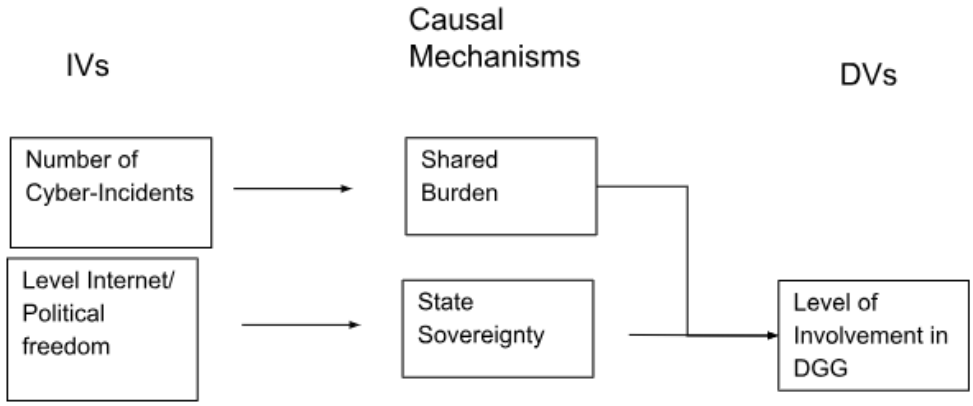

Figure 1.

References

Allee, Todd L., and Paul K. Huth. 2006. "Legitimizing Dispute Settlement: International Legal Rulings as Domestic Political Cover." *The American political science review* 100(2): 219–34. http://dx.doi.org/10.1017/s0003055406062125.

Dahlgren, Peter. 2000. "The Internet and the Democratization of Civic Culture." *Political Communication* 17(4): 335–40. doi: 10.1080/10584600050178933.

Dellmuth, Lisa, and Bernd Schlipphak. 2019. "Legitimacy Beliefs towards Global Governance Institutions: A Research Agenda." *Journal of European Public Policy* 27(6): 931–43. doi: 10.1080/13501763.2019.1604788.

Dragu, Tiberiu, and Yonatan Lupu. 2021. "Digital Authoritarianism and the Future of Human Rights." *International Organization* 75(4): 991–1017. doi: 10.1017/s0020818320000624.

Drezner, Daniel W. 2004. "The Global Governance of the Internet: Bringing the State Back In." *Political Science Quarterly* 119(3): 477–98. doi: 10.2307/20202392.

Glen, Carol M. 2014. "Internet Governance: Territorializing Cyberspace?" *Politics & Policy* 42(5): 635–57. doi: 10.1111/polp.12093.

Jackson Adams, and Mohamad Albakajai. 2016. "Cyberspace: A New Threat to the Sovereignty of the State." *Management Studies* 4(6). doi: 10.17265/2328-2185/2016.06.003.

Jia, Kai, and Shaowei Chen. 2022. "Global Digital Governance: Paradigm Shift and an Analytical Framework." *Global Public Policy and Governance* 2(3): 283–305. doi: 10.1007/s43508-022-00047-w.

Kaska, Kadri, Tomas Minarik, and Henrik Beckvard. "Huawei, 5G, and China as a Security Threat." *Ccdcoe.org*.

https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/ (May 9, 2023).

Lambach, Daniel. 2019. "The Territorialization of Cyberspace*." *International Studies Review* 22(3): 482–506. doi: 10.1093/isr/viz022.

Larionova, Marina, and Andrei Shelepov. 2021. "Emerging Regulation for the Digital Economy: Challenges and Opportunities for Multilateral Global Governance." *International Organisations Research Journal* 16(1): 29–63. doi: 10.17323/1996-7845-2021-01-02.

Lee, Yongjae. 2022. "Can Digital Authoritarianism Deter Political Freedom? : Innovation in Digital Technology and Democratization." *The Korean Journal of International Studies* 20(1): 21–53. doi: 10.14731/kjis.2022.04.20.1.21.

Mueller, Milton L. 2019. "Against Sovereignty in Cyberspace." *International Studies Review* 22(4): 779–801. doi: 10.1093/isr/viz044.

Runde, Daniel F., and Sundar R. Ramanujam. 2021. "Global Digital Governance: Here's What You Need to Know." *CSIS*. https://www.csis.org/analysis/global-digital-governance-heres-what-you-need-know (February 19, 2023).

Sukhodolov, Alexander P., Elena G. Popkova, and Irina M. Kuzlaeva. 2017. "Modern Foundations of Internet Economy." *Internet Economy vs Classic Economy: Struggle of Contradictions*: 43–52. doi: 10.1007/978-3-319-60273-8_4.

Tekir, Gökhan. 2020. "Huawei, 5G Network and Digital Geopolitics." *International Journal of Politic and Security* 2(4): 113–35. https://doaj.org/article/661d8f44eb494359b317f08accbe1d22 (May 9, 2023).

Xinmin, Ma. 2016. "Key Issues and Future Development of International Cyberspace Law." *China Quarterly of International Strategic Studies* 02(01): 119–33. doi: 10.1142/s2377740016500068.

"Freedom on the Net." *Freedom House*. https://freedomhouse.org/report/freedom-net (April 10, 2023).

"Publication Archives." *Freedom House*. https://freedomhouse.org/reports/publication-archives (April 10, 2023).

"Tracking State-Sponsored Cyberattacks around the World." *Council on Foreign Relations*. https://www.cfr.org/cyber-operations/ (April 10, 2023).