The Progression of Chinese Cyber Norms within the UN

Voshell, Leanne

The Progression of Chinese Cyber Norms within the UN

Voshell, L.M. (Leanne)
Asian Studies Research Master
Leiden University
S2438062
30 ECs
23/08/2022

Abstract

For the past two decades, states have been engaged in negotiations concerning acceptable state behavior in cyberspace. Many states have submitted their views on the matter and most recently, cyber norms negotiations have been opened up to the entire membership of the United Nations through the Open Ended Working Group. Chinese representatives have been an active participant in these negotiations since their inception, with their own preferred cyber norms to promote. The success of this promotion, however, has been limited due to several factors. In this research, this attempted norm promotion is examined in detail through primary documentation to assess what these limiting factors entail.

Table of Contents

1. Introduction

In 1996, John Perry Barlow wrote “A Declaration of the Independence of Cyberspace”, to proclaim that “cyberspace does not lie within your borders” (Barlow 1996). The borders he is referring to are the borders of states, and he asserts that cyberspace and the internet do not lie within the jurisdiction of the state. These online spaces were only in use by less than one percent of the world population during 1996, making it much easier to claim that the governments of the world did not have sovereignty over cyberspace. However, in 2021, over sixty percent of the world had access to the internet and these online spaces (Digital around the world 2021). This number is only going to grow with time as further useful functions are incorporated on the internet.

This increase in internet use is also applicable to states themselves, who have been increasingly incorporating e-government infrastructures. Indeed, the United Nations has measured the growing capability of state e-government since the early 2000s with the e-government digital index (EGDI). In 2001, the average worldwide EDGI was measured at 1.62 on a scale of 10. Almost 20 years later, this worldwide average has increased to 5.98 (Ronaghan 2002; UN E-Government Knowledge Base 2021). With such a growth of e-governance, it is not surprising that states have a vested interest in regulating the internet. Perry’s early declaration of cyberspace and the internet as a state jurisdiction free zone has since been rejected by states because of this interest. Outside of e-governance, developments like the internet’s increasing penetration rate, society’s reliance on the internet for daily life, and the increasing threat of malicious use has created a problem too big for states to ignore. This increasing malicious use also includes state use of cyberspace and the internet to carry out digital invasions worldwide, necessitating regulation on state behavior in this fairly new realm.

How these states prefer to define and regulate cyberspace internationally varies wildly from state to state. For example, the United States chooses to define cyberspace as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers”

(Congressional Research Service 2021). The use of "a global domain" in this definition signifies that the United States recognizes cyberspace as a virtual space, akin to land, sea, and space. This virtual space is enabled by the technical infrastructure and tools developed to be used on the internet, but by definition is a space unto itself. This implies that the regulation applied to cyberspace and the internet should be similar to the laws governing other such global domains. This would include current norms for other domains as applicable to cyberspace as well as already established international law.

In contrast, China[1] would define cyberspace in a much different manner. The focus of this definition is on the information technologies and infrastructures that compose cyberspace. In the 2016 Cybersecurity Law enacted in China, clauses including cyberspace are very broad, opting not to define the nature of cyberspace specifically (The Standing Committee of the People's Congress 2016). Instead, this law focuses on information security and the regulation of internet infrastructures allowing information in and out of the state. For China, cyberspace is not a virtual space, but a set of infrastructures and information systems to be regulated based on their physical location as part of a state's territory. Cyberspace is not a domain unto itself but dependent on the physical world to be regulated.

This seemingly necessary regulation of cyberspace and the internet was brought to international attentions during the early to mid 2000s. By that time, the developers of the internet and associated businesses had already been developing practices of standard behavior regarding the internet and cyberspace for two decades. For states, these practices translated to norms in which all parties recognize which behaviors are acceptable and which are not within a given subject matter. State-developed and supported concepts of standard behavior online were far behind these privately developed norms, and this required rectification in the eyes of some states. These included Russia and China, with the former submitting a resolution to the United Nations (UN) to establish a forum negotiating multilateral cyberspace norms. It passed in 2003,

[1] The definition of 'China' in this paper refers to the Chinese government and its representatives internationally. It does not encompass the views or ideas of groups outside of the government, since their views will not be represented within the UN internet forums.

establishing the Group of Governmental Experts to work toward negotiating acceptable state behavior in cyberspace.

During these forums, each participating state can share its domestic best practices, policies, and norms regarding acceptable behavior in cyberspace. Generally, once a norm has been incorporated within international institutions, it is very difficult to overturn. So those nations that promote their norms early are more likely to find success, motivating states to compete to validate a state's preferred norms. Many states are attempting to use these forums to influence the development of these norms, including the United States, Russia, China, and the states of the European Union. In this thesis, the research focus will be on Chinese-promoted norms within these UN based forums to develop acceptable standards of state behavior in cyberspace. The ultimate goal of this research is to assess the progress that the promotion of these norms has made within these forums through close reading analyses of consensus documentation, submitted documents, and relevant domestic policy, among others.

First, a few chapters will be dedicated to the background necessary to understanding the outcome of the analysis undertaken in this research. Norms, while briefly mentioned and broadly defined already, will be explored first to give theoretical background and context for the reader. Next, this research explains the usefulness of the UN as a forum for Chinese cyber norms and some of the domestic policies that underlie the norms that China promotes internationally. A detailed history of the UN cyber norm forums will be included following this, giving the reader background on the overall process before specifically analyzing Chinese norms within this process. The analysis, preceded by methodological considerations, will include a chronological progression of Chinese-promoted norms and a discussion of these implications. This thesis draws the conclusion that, while some Chinese-promoted norms have found acceptance on the international stage, key norms required for overall internalization of its norms "package" have fallen far short of the acceptance needed.

2. Norms and Norm Entrepreneurs

Within International Relations, it is "generally agreed" that norms are defined as "a collective expectation for the proper behavior of actors with a given identity" (Finnemore 1996)[2]. These norms are meant to regulate the behavior of national entities and representatives interacting on an international level, constraining the actions that can be taken and regulating the interactions that may be expected from a given situation. The development of these shared expectations of behavior is meant to encourage the relative order and stability that is present on the international stage (Katzenstein 1996; Sunstein 1997; Wendt 1992 from Finnemore and Sikkink 1998; Adamson et al. 2020). The theory concerning why these norms emerge has been explored by quite a few academics. For example, Cass Sunstein coined the term "norm entrepreneur" and "norm management" in 1996 to explain why and how desirable behavior can be encouraged through regulatory measures (Sunstein 1996). More recent research, however, focuses on the concept of the norm "antipreneur" and the contestation of the norms already present. This theory focuses on the entrenched norms, as well as the actions that actors may take to maintain the precedence of the norm within its place in society (Bloomfield 2016). One of the most frequently used is Finnemore and Sikkink's (1998) theory of norm life cycles. It is this theory of normative life cycles that this thesis uses to provide a frame to analyze how much influence Chinese cyber normative efforts have had in the UN.

Finnemore and Sikkink's (1998) normative three-stage life cycle is fueled by the actions of norm entrepreneurs. These norm entrepreneurs can originate from many organizations, including non-governmental organizations, international organizations, states, non-profits, or businesses. This is not an exhaustive list, considering that there are many organizational structures that could benefit from specific norms becoming codified and internalized internationally. However, states will be the focus of the analyses provided here, since the United Nations is a multilateral organization focusing on the participation of states. Especially within the negotiation of cyber norms, which was primarily a private enterprise from its inception, states are relatively new norm entrepreneurs and must compete with the norms already established by other norm entrepreneurs, as well as the preferred norms of other states. In the case of states as

[2] See also; Katzenstein 1996; Klotz 1996 from Finnemore and Sikkink 1998; Broeders et al. 2020

norm entrepreneurs, preferred norms are always developed as domestic policy first. It is only after domestic development that these policies, now turned norms, will be promoted internationally. It should also be noted that the state, itself, is not one monolithic entity. It is composed of several parts of society, government, and business who would all like to influence domestic policy. Especially within the government of a state, interpretations and enforcement of policy differ between officials and bureaus alike. When discussing domestic state policy, I personally prefer to use the plural because of the diversity of views within a given state. Within the discussions of this research, however, the state will be referred to as a singular due to the nature of its representation within the UN. The forums under discussion are concerned with the domestic policies promoted at the international level.

Now, regardless of how in depth these domestic policies have been discussed within the state, the representation of these states relies on a single representative presenting the policies of their nation on an international level. Of course, there are many staff from every participating state present within the UN, but forums such as the Group of Governmental Experts (GGE), the Open Ended Working Group (OEWG), and even the General Assembly rely on one representative to vote and lead the negotiations for the state according to its domestic policy. As representation for a state on the international stage, these appointees are always part of the governing body of that state, since that is the authority that the UN represents. These representatives debate and negotiate based on official government policy, regardless of what the domestic discussion surrounding it may be. These domestic state policies are what states hope to promote, pushing their preferred policies through the norm life cycle and into official UN guidelines for state behavior. As one of many norm entrepreneurs, China also hopes to influence the international cyber norm standards through its own domestic policy. Since the issuance of China's 2010 White Paper concerning the internet, China's international positioning regarding cyber issues has remained largely the same (Full Text 2010; China's Submissions 2019; A/69/723; A/66/359). As concepts are elaborated more within China's academic and policy communities, specifics are added to the international by-line.

In order for states to successfully become norm entrepreneurs, domestic policies must first be introduced on the international stage in the first stage of the normative life cycle, which

Finnemore and Sikkink (1998) call “norm emergence”. During this first stage of emergence, a state will promote its domestic policies as a preferred norm in the role of a norm entrepreneur to the general consciousness of other states through information exchange. The goal of the norm entrepreneur in this first stage is to persuade as many states as possible that the entrepreneur’s domestic policies are in their best interest to adopt as international norms. This idea of ‘best interest’ sounds like states are expected to make the choice that makes the most sense. Certainly, realism-based rational choice theory is one way to explain why states choose to adopt certain norms. Originally based off Adam Smith’s work on political economy, the application of this theory within international relations assumes that states and associated actors are consciously making choices based on rational, strategically sound thought (Boudon 2003).

However, this is not always the case within international relations. As researchers, it is still important to note that these representatives of state government are still human, affected by emotions, culture, and experience. What may seem like the best choice to one state may be ranked very differently as a choice for other states. For many, this recognition has caused many academics to turn toward constructivism as a lens to interpret decision making within international norm emergence and adoption. This is explained through the “logic of appropriateness”. The definition of appropriate depends heavily on the identity and experiences of the actor in question, causing them to make behavioral decisions based on experience (March and Olsen 1996).

The decision to accept an emerging norm usually relies on a mix of both theories, where each state must balance what will yield the most benefit while considering the lived experiences of that state. This mix of decision making is often translated into what states call their national priorities. These priorities are informed by both strategic thinking as well as lived experienced of that nation, simplified for the international stage in the form of norms. By convincing other states that the entrepreneur state’s domestic norms are best to adopt on the international stage, it solidifies the achievement of its national priorities internationally. This, of course, does not guarantee the achievement of those same national priorities domestically, but this is beyond the scope of this research. Attempted efforts at norms persuasion in this first stage are often carried out through various international organizations and are subject to specified language to frame the

issue in a way that other states will identify with. After all, the emergence of the norm within Finnemore and Sikkink's theoretical cycle depends on the other states in this equation and requires the acceptance of these states to proceed to the second stage of the norm life cycle. Without adoption and implementation from other states, this emergent norm remains a domestic policy and moves no further.

However, emergent norms that do find success on the international stage reach the second stage of the norm life cycle, known in Finnemore and Sikkink's theory as a "norm cascade". During this cascading stage, growing adoption of the promoted norm signifies its rising popularity, leading to a cascading international adoption of the norm entrepreneur's promoted policies. As with the first stage of norm emergence, a norm cascade can fizzle out if it reaches a ceiling on the number of states that are willing to adopt this norm. This rate of cascade depends on the circumstances in which the previously emergent norm was promoted, leading other states to adopt the cascading norm for various reasons. In some cases, it will be adopted to legitimize the state that has decided to incorporate this norm within its regulatory landscape because of the positive reputation of or relationship with the norm entrepreneur. In other cases, these norms will be adopted by states because of identification of shared values within this norm. This does not encompass all the possible reasons why states would adopt a norm, considering that very few theories are able to incorporate every single case into their conceptualization.

If the cascading norm is adopted by a large majority of states, the promoted norm then reaches the third stage of the norm life cycle. This widespread implementation is known as "norm internalization". If a promoted norm reaches this third stage, it is often taken for granted as a constant (Finnemore and Sikkink 1998). One such example of an internalized norm, in relation to states, is the concept of borders. All states accept that borders are necessary to maintain their nation, even if there are conflicts over where these borders should be. Regardless of these conflicts, it is still agreed that there must be a dividing line between states within our international system. This normative idea dates back to the 1648 Treaties of Westphalia, in which states agreed to recognize the authority of other states over a given territory. Over three hundred years later, this norm has since been internalized and often taken for granted.

The creation and establishment of norms is not a simple process and is, largely, misunderstood. Norms are meant to be dynamic, evolving as need be to encompass the changing landscape surrounding these norms. This would mean that the adoption of norms from one state's or very few states' domestic policies would inherently be a negative development. Currently, the cyber norms negotiation process currently relies heavily on previously established precedent in the UN and lacks flexibility. Instead, norms that most clearly match the real-world needs of cyber regulation would be the most prudent to adopt, even if that means pulling from the domestic policies or best practices of multiple states. With rapidly developing technological abilities, the dynamic nature of norms would be able to help regulate as needed, oftentimes being codified into law once these norms are internalized at a certain level. This use of norms in the negotiations over regulating cyberspace would, theoretically, be able to create consensus on cyber norms before establishing these norms within more concrete institutional structures. It would signify who agrees with what norm and the interpretations they have of that norm before firm international legal codification. This also allows for flexibility in regulation because states have the power to adjust normative measures to the context in which they are functioning.

However, prospective norm entrepreneurs often misunderstand the purposes behind establishing emergent norms. States attempt to develop norms as a set of guidelines or principles modelled on domestic policy to establish fixed guidelines on state behavior. These norms are promoted on the multilateral level to be accepted or rejected by other states, many of whom assume that norms are not subject to change once established (Finnemore and Hollis 2017). In reality, norms should be dynamic and process-focused. Norms should be able to change their meaning or interpretation based on the current circumstance, especially considering the rapid development of internet technologies. This also means that norm discussions and forums would need to monitor a norm's usefulness over time and evaluate needed changes. This indefinite negotiation process is important to develop useable norms.

The flexible nature of norms to adapt is one of the most important aspects of a norm, but this concept is often missing from multilateral discussions on cybernorms. Instead, stagnation is normal in the multilateral cyber norms process. Norms developed in the UN process are products of packaged behavior negotiated in a closed forum by a small number of states (Finnemore and

Hollis 2017). These norms are then expected to promulgate world-wide even though not all parties subject to these norms were involved in their negotiation process. In addition, they are labeled as "voluntary" and "non-binding" without guidance outside of the "goal-oriented obligation" prescribed in the norm, which in a context where the stakes are high could be helpful. Unfortunately, there is a lack of trust and solidarity in the regulatory landscape of cyber norms, so states are very unlikely to implement these norms in a purposeful way until a measure of trust is present (Adamson 2020). This is likely due to the state focus on norms as a product rather than a process. States negotiate through their preferred norms, setting an agenda before the negotiation process begins. This closes off possibilities of flexibility within cyber norms because each state is negotiating toward a prescribed outcome.

A large part of acceptance rests on the who, where, when, and how these norms are incorporated (Finnemore and Hollis 2017). Is this norm accepted by a state that holds a positive or negative standing within the international community? According to Finnemore and Sikkink (1998), there is technically no such thing as a 'bad norm' based on the viewpoint of those who are promoting the norm, but the perception of other states can certainly cast a negative light. For example, there is the idea of 'norm regression', which is defined as the spread of norms that are seen as a degradation of norms by other states than the norm entrepreneur (McKeown 2009 from Deibert and Crete-Nishihata 2012). This idea of regression is entirely subjective and open to interpretation. Was the forum where the norm was created seen as a legitimate norm making body?

Here, discussion will focus on the UN as the negotiating body to create cyber norms. The UN is the foremost international organization with the largest membership worldwide, which allows for a large platform, widespread consensus, and largely legitimized consensus documentation. But, if legitimacy for emerging norms cannot be found within a certain forum, then the norm entrepreneurs will often find a forum that will better promote their emerging norms. Consensus documents issued by the UN GGE, although originally proposed and established at the behest of Russia, largely promoted the cyber normative agenda of the United States and like-minded friends (Broeders et al. 2020). This forum only had a small number of participants working toward the establishment of cyber norms. After each successful forum,

these representatives published a consensus document detailing the progress that had been made in these negotiations (Fact Sheet 2019). However, this format means that many states are not able to meaningfully participate in this process and the negotiated cyber norms produced by the GGE process are not universal. Because of this exclusion of states, the growing urgency of cyber norm negotiation, and the failure of the GGE to come to a satisfactory consensus in 2017, Russia proposed and established the OEWG for cyber norms in 2019. Because of the increased importance of cyber norms, the GGE lost legitimacy by limiting participation and losing progress. In order to make more headway for emergent norms that may not have been legitimized through the original GGE process, a new forum with more participation was needed (Finnemore and Hollis 2017).

In addition, the framing of the proposed norm is important as well. The framing of the norm has long term consequences, as these terms can often be interpreted differently based on the context and the promoter (Finnemore and Hollis 2017). The dominant norms surrounding cyberspace at the time of writing are often tied to human rights and the guarantee of open internet access (Cho et al. 2017). A large portion of states that identify themselves as human rights promoters will often find this framing the most convincing because of their values. However, many of the emergent norms in cyberspace focus less on human rights and more on the ability to control content and create a secure cyberspace. This definition of secure cyberspace varies widely, but it certainly matters how norm entrepreneurs frame it as well. Will cyber norms focus on avoiding possible cyberspace militarization or protect the technical aspects of the internet? Is information a threat or an asset to the security of a state? Different norm entrepreneurs will have different definitions of key terms that are used in negotiations and different views on what the real problems of cyber norms are, as well as how to tackle and word these issues (Slack 2016; Finnemore and Hollis 2017). These, and many other questions, determine the rate of adoption when it comes to norms. If they are seen as legitimate and worth adoption by states that have not previously implemented these norms, it is more likely that a norm will find success than norms that do not have legitimacy and agreement when it comes to their content.

This process of norms creation has been slow going within multilateral deliberations over cyber norms. With time, cyberspace has come to control a large portion of innovation, economic activity, communication, and data storage, among others. The internet and cyberspace are now essential to everyday society and this interdependence creates an increased risk of vulnerabilities. The uncertainties associated with this interdependence hardly encourage states to trust the process. Instead, states are unwilling to create codified boundaries with little hope that others will follow. This, in combination with the wide variety of viewpoints and cyberspace infrastructure development levels, makes the creation and promotion of cyber norms a complex, and often contested, challenge (Nye 2017; Pawlack 2016; Adamson et al. 2020; Broeders et al. 2020). These norms will also need to regulate an enormous user base. With low barriers to entry for the internet, almost anyone can become a cyber actor with the right equipment and knowledge (Ruhl et al. 2020). How will these norms be enforced within such a large population? In addition, the creation of cyber norms does not take place in a vacuum. The political debates and tensions that are present on the international stage will still exist within these negotiations and influence the stances that states take on these issues.

As alluded to, there are largely two different sides to the cyber norms debate that started emerging on the multilateral level with the first UN GGE in 2004 (Lantis and Bloomberg 2018). On one hand, there are the United States and those states that promote the idea that the internet should remain as unregulated as possible to maintain an "open, secure, stable, accessible, and peaceful ICT environment". This phrasing that has been included since 2013 in all UN cyber norms documentation (A/68/98; A/70/174; A/AC.290/2021/CRP.2; A/76/135). This wording is quite close to the phrasing used in the United States published International Strategy for Cyberspace from 2011, which precedes its inclusion in the UN cyber norms process. This document describes the best future for the internet as "open, interoperable, secure and reliable", which shares many of the same concepts as the previous UN based phrase (International Strategy 2011).

The US policy viewpoint is that cyber norms should protect cyberinfrastructure and networks from major attacks carried out by non-state actors (Cho et al. 2017; Flonk et al. 2020; Henderson 2021). These states also hold the belief that established international law and norms

are enough to regulate cyberspace. Their understanding is that there needs to be development in the adoption of these norms as well as in how exactly international law and these norms apply in practice. Indeed, many of the norms in the 2015 GGE consensus document reflect and reinforce the ideas and values of existing international law (Tikk et al. 2018; Adamson 2020). Overall, it is the United States, 'like-minded' friends, and other actors based within these states that have established most of the cyber norms that govern the internet so far, and they would like to continue this dominance (Flonk et al. 2020).

On the other hand, there are China and Russia along with associated states who promote the idea of information security. The belief of these states is that the focus of cyber norms should be on the protection of information and cyberinfrastructure from outside interference. The 'free flow' of information that is seen as desirable by the US-led contingent is seen as a threat to the domestic stability and security of states promoting information security (Tikk et al. 2018; Cho et al. 2017; Lantis and Bloomberg 2018; Segal 2020). Cyberspace itself is seen as having larger political connotations and is often conceptualized as an information space that needs to be regulated. Indeed, the UN seems to agree with this idea that the internet and cyberspace encompass more than just technical aspects, now including social and economic implications (Haugen 2020). Monitoring and controlling cyberspace, therefore, is essential to the security of the state.

Additionally, these states have expressed that the application of international law to cyberspace poses a threat. This threat would hypothetically stem from two sources; the application of current international law to cyberspace and the inability of current international law to specifically regulate cyber issues. Although there would be guidelines present for how states should conduct themselves in cyberspace with the current international law, these states argue that it is not specific enough to prevent interpretations that allow for cyber threats. Without guidelines specific to cyberspace, many states will use interpretations of current international law to militarize cyberspace for use in conflict while remaining compliant with international obligations. This includes legitimizing self-defense measures after a cyber-attack, which would allow for the potential use of retaliatory strikes against cyber espionage or attacks. This is something that states such as both China and Russia would like to avoid, considering that they

often use these tactics and would not like physical retaliation to a cyber-attack to be legitimized (Cho et al. 2017; Segal 2017; Sukumar 2017; Slack 2016; Tikk et al. 2018; Stadnik 2019).

For this reason, they prefer the creation of a separate international treaty or legal document that would outline new international law applicable to cyberspace. State control of the internet and cyberspace is necessary, and the norms promoted by this contingent reflect this, striving for the legitimization of state control over the internet (Flonk et al. 2020; Henderson 2021). Whereas the former camp has their norms largely enshrined, China and like-minded friends are heavily focused on the creation of forums, such as the GGE and OEWG (both of which were initiated by Russia), in order to have a platform to promote their normative views and keep the opposing side, namely the United States, in check (Cho et al. 2017; Flonk et al. 2020; Segal 2020).

In addition, there is a third side emerging who are considered 'swing states'. This group is mostly composed of developing countries that have remained noncommittal towards the negotiations of cyber norms. These states have not necessarily relegated numerous resources to these negotiations, but tend to pursue equal access to information and technology that will allow them to become more technologically developed. Instead of focusing on political and normative agendas, priority is given to overcoming the 'digital divide' that has emerged between powerful ICT countries and those with less ICT power (Basu et al. 2021; Tikk et al. 2018; Cho et al. 2017). However, there does seem to be some sort of agreement between states; the imperative to protect cyberspace and its associated infrastructures from activities that interfere with security, economy, and finance. Considering this apparent agreement, normative disagreements must stem from states' interpretations of necessary actions to create stability (Cho et al. 2017; Stevens 2012).

Of course, State-led cyber norms negotiations are still in the beginning of their life cycle and require time to develop shared common understandings. Right now, technology is moving much faster than it can be regulated through normative and institutional fora. In addition, the actors and institutions who are influencing the internet are changing constantly. Because of this, states often lag in their understanding of developing technology and the external ramifications of regulatory technology policies (Maurer 2019; Nye 2018; Ruhl et al. 2020). In contrast, there is

already a large network of norms that have been developed over time by both State and non-State actors. These include national regulations, professional standards, political agreements, and technical protocols that have already developed normative expectations to cover a series of diverse issues within cyberspace, without a single, shared context (Finnemore and Hollis 2017). Multilateral negotiations in the UN have, so far, largely ignored the previous work, influence, and, at times, dominance that other public and private actors have had on the creation of cyber norms (Broeders et al. 2020). These groups often address non-traditional security issues that are not prioritized by multilateral cyber norms negotiations, but are instead prioritized by other important non-State actors that are generally relegated to 'observer' status within the UN (Cho et al. 2017).

This heavy influence to keep the internet as open as possible led to disregard internationally of the state's role within cyberspace. For a long time, the only international deliberation on cyber norms had to do with the technological protocols that built the infrastructure, largely controlled by those with technical expertise. However, with the advent of an internet that controls a large portion of the economy, infrastructure, information, and security, many states only now have a more vested interest in the political ramifications that the cyber realm presents. Additionally, the internet facilitates rapid information spread across borders, providing unique challenges to sovereign states that may be attempting to enforce domestic policies in cyberspace. The 'benign neglect' that had characterized the treatment of states' regulation of the internet became something requiring attention (Basu et al. 2021; Gill 2020; Klimburg 2017; Segal 2016; DeNardis 2014; Deibert 2013; Betz and Stevens 2011 from Broeders et al. 2020; Arsene 2016).

In addition, increasing investments in the development of defensive and offensive cyber capabilities alludes to the need for regulation of state behavior when using those capabilities ("UN GGE and OEWG" Digital Watch 2021; Goel 2020). These capabilities and cyber activities remain largely unknown to those outside of the states themselves. There is a distinct lack of transparency around the beliefs that states hold toward shared expectations of appropriate behavior in cyberspace in general and militarily (Ruhl et al. 2020; Maurer 2019). One of the purposes of the multiple cyber norms fora in the UN is to promote the sharing of these views in

order to better establish the ‘rules of the road’ when it comes to offensive and defensive uses of cyberspace. However, revealing expectations and beliefs regarding these developed capabilities is not to most states' advantage right now, due to the lack of trust that remains evident in cyber norms negotiations (Gill 2020; Adamson et al. 2020; Goel 2020).

As the premier international organization with the widest membership role, the UN is a logical choice for the deliberation of cyber norms on a multilateral level. Although there have been many other efforts to create norms outside of the UN,[3] much of the current State cyber norm creation is currently focused within UN auspices, especially the GGE that has convened several times since 2004 and the OEWG, which was newly established in 2019.

[3] The following discuss such non-UN forums in greater detail and can be found in the references; Epstein 2013 (Internet Governance Forum), Hoffman 2012 (Internet Engineering Task Force), Klein 2002 (Internet Corporation for Assigned Names and Numbers), Almeida 2014 (Net Mundial)

3. China's Choice of the UN

The UN is also the premier choice for cyber norm negotiation by the government of China (Flonk et al. 2020; Tikk et al. 2018; Cornish 2015). As an international organization in which China holds a substantial position, the UN is seen as the best possible path for Chinese domestic internet policy to find acceptance and to emerge as international cyber norms. In fact, in 2014, the government of China moved to take a more public role to 'reform the international system and global governance' and has only been increasing this prerogative, even going to publicize their goal of becoming a global cyberpower (Kanis et al. 2017). However, participation in the UN and the international system in its current form has helped to propel China to the position of power it now enjoys. So, this reformation is not necessarily meant to be a full overthrow, but instead a recalibration toward the national interests and priorities of the Chinese government (Yang 2020; Arsene 2016).

This attempted international reformation in the favor of China has been happening for quite a while, but with the public acknowledgement of these goals, it transitions to a more public recognition toward the priorities of China's current government. Within the UN, China's priorities are largely issue dependent; if the international norms are contrary to the national interest of the Chinese government, it is much more likely to work on reforming that part of the international order through the attempted promotion of values that China would rather see as the norm. This especially applies to the concepts of sovereignty and non-interference; the government of China wants to participate on the international stage while still maintaining strict sovereignty to prevent interference within its domestic sphere (Yang 2020; Weiss and Wallace 2021; Creemers 2021).

Based on this knowledge, the high priority that the government of China has placed on influencing the outcomes of internet governance and cyberspace norms on the international level means that it considers these norms to be important to China's national priorities. Since cyber norms are such a new area of multilateral normative debate, new norms face high competition with the current de-facto normative rules (Yang 2020). The security that is needed for the continuation of Chinese state control of cyberspace and the centrality of the cyber norm debate to

current events means that it is highly unlikely that China will be flexible now or in the future regarding what it sees as essential to ensure the success of its national interests and priorities (Zeng et al. 2017). Considering that the proliferation of Chinese cyber norms faces huge obstacles in the form of opposition from the dominant normative and technical practices promoted by the United States and like-minded friends as well as from concerns about China's less than savory online censorship practices, the promotion of cyber norms has a certain priority (Yang 2020; Segal 2020).

This is especially true due to the focus on the idea of internet freedom and openness that is heavily linked to the normative notions of human rights and freedom of expression. This directly opposes the norms that China would like to promote, considering that China's hope is to pursue information security through internet filtering as needed by government standards (Carr 2016; McCarthy 2015; Powers and Jablonski 2015 from Budnitsky and Jia 2018). If the representatives of the Chinese government can successfully promote Chinese domestic internet policies to international cyber norms within UN forums and have those norms accepted by the General Assembly, it will be one step closer to acceptance of more restrictive cyber norms. In fact, China supported Russia in establishing the first GGE to 'examine the existing and potential threats from the cyber-sphere and possible cooperative measures to address them' (A/RES/58/32; Lantis and Bloomberg 2018).

Additionally, the UN itself or a body formed within UN auspices are examples of forums that China would like to see as the main governing body for many aspects of internet governance. Currently, many technical aspects of the internet are controlled by the US-based internet Corporation for Assigned Names and Numbers (ICANN). It is not fully under the control of the US government anymore, after the 2014 announcement of the transition from US government oversight to an international multistakeholder model (Administrator of the DNS… 2014). Even so, Chinese representatives have stated at the latest round of negotiations that "the current distribution and management of critical internet resources pose security threats to the functioning of critical infrastructure" and would much rather have the governance of the internet in the hands of the United Nations and a "truly independent international institution" (Gavrilovic 2019; Kaska and Tolppa 2020). Whether this is a reference to the dominance that the United States enjoys

with internet infrastructure or the militarization of cyberspace, China does not want governance of the internet to be determined by non-governmental representatives, which is the core of the currently normalized multi-stakeholder governance. Instead, China would like internet governance to be focused on the multilateral level, where the states themselves decide how the internet will be governed (Lantis and Bloomberg 2018; Segal 2020; Budnitsky and Jia 2018). Since the UN is, mainly, a multilateral institution that works with "observers" from NGOs, businesses, and other organizations, it is the platform that China would prefer.

Instead of applying current international law already present in the UN to regulate cyberspace, China would like to create entirely new rules and forums to manage the governance of the internet within UN forums. This would be based on the "code of conduct" developed by the countries involved with the Shanghai Cooperation Organization (SCO) and introduced to the UN several times (Kaska and Tolppa 2020; Arsene 2016). The countries involved in the SCO include China, India, Kazakhstan, Kyrgyzstan, Russia, Pakistan, Tajikistan and Uzbekistan. Afghanistan, Belarus, Iran, and Mongolia also participate, but as observers interested in full membership. The concepts in the code of conduct reflect largely the norms that China would like to promote concerning cyberspace: to respect sovereignty and territorial integrity, ban hostile actions or aggression through the use of cyberspace, cooperate on solving crime and terrorism in cyberspace, create a democratic and multilateral internet management system, and promote the role of the UN in the development of cyber norms (A/66/359; A/69/723; China's Submissions… 2019).

One of the most highlighted aspects of this code of conduct is the desire to outright ban the use of cyberspace for aggressive actions, which refers to the development of military actions in cyberspace that most states with cyber capabilities are engaging in. One of the most prominent reasons for this ban is the fear of international law legitimizing cyberattacks and the following retaliation. In order to argue against the full applicability of international law in cyberspace, China stated that by allowing IHL and Article 51 - the laws governing armed combat and a state's right to self-defense- to govern cyberspace, the possibility of a cyberwar becomes legitimized (Tikk et al. 2018; Segal 2020; Stadnik 2019). These disagreements on the possible interpretations of international law in cyber space caused the failure of the 2017 round of GGE

cyber norm negotiations (Segal 2020; Tikk et al. 2018;). So, the Chinese government believes that a new set of rules and norms should include an outright and total ban on force in cyberspace (Cho et al. 2017; Tikk et al. 2018).

4. Chinese Internet Policy

So what kind of norms and rules does the government of China want to promote at the international level? This was, in part, introduced with the code of conduct briefly discussed earlier. As previously mentioned, the basis for these proposed international norms is rooted in domestic concerns and approaches to internet governance (Weiss and Wallace 2021; Finnemore and Hollis 2017). Much of international participation depends on the concerns that states have domestically and are always meant to provide a positive global effect through their actions. Rather, China transfers its domestic policies to the international level to reflect the state of its national priorities (Zeng et al. 2017). Cyber norms are no exception to this. China developed extensive domestic cyber policy much earlier than most nations with advanced cyber capabilities to remedy the perceived insecurity that access to the internet provides in states that prefer the ability to control which information is accessible.

Although the internet was introduced in China in 1994, it was not until later that China prioritized shaping global internet governance according to Chinese policy and norms (Shen 2016). At first, the focus was on the domestic, building up the infrastructure needed to make access to the internet available as well as developing domestic information security regulations and internet infrastructure. Governments like China and Russia recognized that the internet had the power to greatly change the global political landscape, especially since it was seen as a threat to the primacy of multilateralism and state sovereignty (Lantis and Bloomberg 2018). As highlighted before, China belongs to the contingent that believes free access to uncontrolled information through domestic internet connections is a potential threat to the security of the nation. It is not a mainly technical space, but an information space and resource that must be under the scope of government influence. To this point, the major belief is that [dis]information campaigns from external sources are a threat to state sovereignty, interfering with the way that the current government of that state chooses to administer the country and internet controls are essential to maintaining political stability (Lantis and Bloomberg 2018; Yang 2020; Kaska and Tolppa 2020).

To a certain point, this is a valid concern. The advent of the internet was seen as a liberating moment, giving users free access to information, international communication, and other perspectives. There was a slew of articles that spoke about the hopes and beliefs that the internet would bring organized protest and democracy to countries that were ruled by an authoritarian government. However, this belief was not necessarily founded on solid ground. Since the introduction of the internet in China, regulations were (and still are) implemented to protect Chinese information systems, especially 'state affairs, economic construction, national defense, and the most advanced science and technology' (Scott and Craig 2014). These regulations, first published in 1994, defined the level of risk for information systems nationwide.

However, the definition of what constitutes a risk is quite broad, and therefore includes a large swathe of China-based companies and websites present on the internet. Later, this definition grew to resemble an expanded version of what most would call critical information infrastructure (CII), including "public communication and information services, power traffic, water resources, finance, public service, egovernment… media, healthcare, cloud computing, and big data providers" (Segal 2020). It was only later that the idea of national security was listed as potentially affected by various factors such as including 'instability of national politics, public information resources, defence, ethnic unity, … strength of the economy, science, and technology' (Scott and Craig 2014). In fact, like many laws and regulations published in China, this definition could be extended to so many areas of the internet that anything could potentially be impactful to national security.

To secure its cyberspace, China asserts that it is necessary to maintain strict, State-centric control. The administration of Xi Jinping, the current President of China, prioritized the establishment and implementation of several domestic governmental bodies and regulations especially for cyberspace. These form a complicated web of strategies, laws, measures, regulations, and standards focused on infrastructure and data. Two of the most highlighted examples of these are the Cyberspace Administration of China and its associated bodies, which control the cyber security of China's internet systems as well as content control, and the 2017 cybersecurity law, which is focused on the protection and localization of Chinese data as well as national security interests in cyberspace (Cho et al. 2017; Creemers 2021; Segal 2020). Since the

internet has become available to Chinese citizens, usage has grown exponentially due to technological advancements allowing increasing numbers online. However, this population has not experienced a largely unregulated cyberspace like much of the world. Instead, internet traffic is routed through a limited number of computers, which then can be used to monitor and censor internet traffic (Lantis and Bloomberg 2018; Scott and Craig 2014).

In addition, China has mandated the use of Chinese IP and promoted the development and implementation of native Chinese technologies within domestic internet infrastructure to mitigate the risks that outside infrastructure and information can promote (Scott and Craig 2014; Segal 2020; Tikk et al. 2018). This fear was confirmed when the PRISM scandal broke. PRISM was a program run by the United States' National Security Agency (NSA) that actively sought out and stored private data from the internet for intelligence purposes. It was only halted when Edward Snowden, a private contractor working with the NSA, leaked the extent of this program's data mining to the media.[4] This only served to prove that technologically developed countries like the United States will use their dominant technical position to gain information.

Considering that the ability to control all parts of the internet through state power is not seen as an acceptable norm by most states, it is necessary for China to promote and reframe its domestic policies on the international stage (Yang 2020; Basu et al. 2021). The most highlighted policy that China is pushing to become an international norm is the concept of 'cyber sovereignty', which is considered the core of the government's cyber policy. First described in a 2010 white paper on the internet, this concept prescribes that every state should determine for itself the level of regulation that its regulators deem necessary for a secure and uninfluenced cyberspace, including strict government control if necessary, without any interference or condemnation from outside states (Full Text… 2010). China argues that the internet is no different than other communication technologies, such as radio or television, which are already considered under the jurisdiction of states within their borders. The adoption of cyber sovereignty on the international stage would allow for increased state cyber control for the sake of maintaining the states' vision of domestic social and political order in a space that has been

[4] For more information on the PRISM scandal, please see the referenced articles released by The Guardian and The Washington Post with the previously leaked information

largely seen as “free and open” for the majority of its existence. Especially promoted as an alternative that will allow for independence while developing digital infrastructure, cyber sovereignty does seem to resonate with some states (Yang 2020; Kaska and Tolppa 2020; Arsene 2016; 2018; Segal 2020; Tikk et al. 2018; Budnitsky and Jia 2018).

Indeed, a report published by Freedom House states that at least thirty-six governments have received private ‘new media and information training’ from representatives of the Chinese government (Lantis and Bloomberg 2018). At the very least, several other countries are approving of China's internet censorship practices enough to request help introducing them into their own cyber landscape. Businesses have already increasingly capitulated to the demands of the government in China regarding cyber/ internet sovereignty to gain access to the Chinese market (Kaska and Tolppa 2020; Broeders et al. 2020). In 2013, the UN general assembly agreed to ‘apply sovereignty to the cyber domain and recognize state jurisdiction over information and communication technology (ICT) infrastructure’ (Cho et al. 2017). In fact, the perceived security threat of an unsecured internet is starting to resonate internationally. For some, this indicates that both sides of the cyber norms debate agree that cyberspace cannot be left unregulated (Lantis and Bloomberg 2018).

5. The UN Process

The UN based cyber norms negotiations process began in 1998 when Russia introduced a draft resolution to the UN General Assembly addressing "developments in the field of information and telecommunications in the context of international security" (A/RES/53/70). The UN General Assembly, International Telecommunications Union (ITU), First, Second, and Third Committee, within the UN have all discussed cyber norms, but this process is particularly focused within the Group of Governmental Experts (GGE) and Open Ended Working Group (OEWG) mandated with discussing the cyber landscape, negotiating norms, and recommending solutions (Henderson 2021).

5.1 GGE

Within the UN, the negotiation of cyber norms was institutionalized in a single process through the GGE to avoid the confusion of different streams within the UN (namely, the First and Third Committee) and to provide a forum for 'purposeful action' regarding possible cyber regulations (Henderson 2021). This forum is based on 'equitable geographical distribution', with the permanent members of the UN Security Council automatically filling the first five seats (China, France, Russia, UK, USA). In the first round of the GGE, only 15 seats were available to member states, but since then this number has expanded to 25. After the first five seats, the rest are allocated by request, lobby, or assignment based on interest.

After seats are assigned, experts are sent to the GGE as representatives of their respective countries. In the beginning of the process, the background of these experts centered around technical knowledge, diplomatic knowledge, or knowledge of information security. As the process has developed, the knowledge base of these representatives has shifted toward arms control and nonproliferation. In order to allow for 'frank discussion', these expert sessions are closed door, with no available public summaries or observers allowed ('UN GGE AND OEWG', Digital Watch 2021). Of course, countries and their representatives may choose to publicly post comments and documents regarding their participation in these GGE sessions, but this is up to the discretion of those involved.

Beginning in 2004, the GGE has consisted of six different iterations, of which four have been able to reach a consensus. The 2010, 2013, and 2015 GGEs achieved three different things. The first consensus, in 2010, established the threats that were developing in cyberspace, stating that 'existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century' (A/65/201). The second confirmed that international law can be applied in cyberspace. In addition, the GGE was able to establish rudimentary guidelines to prevent misperceptions regarding ICT disruptions and important themes for future work on cyber norms, including common understandings of acceptable State behavior, practical cooperation, confidence building measures, and capacity building measures. The third consensus further developed agreement on aspects of cyber security and, most importantly, established eleven non-binding norms that were generally accepted, forming baseline norms to work forward from in determining how international law could apply in cyberspace. These norms affirmed that the UN Charter was applicable in cyberspace, including State sovereignty and jurisdiction as well as human rights in cyberspace, and noted that these norms were derived from already existing international law (Broeders and Cristiano 2020; Henderson 2015, 2021; Basu et al. 2021; Cho et al. 2017).

The two iterations of the GGE that were unable to reach consensus were the first and the fifth, taking place in 2004 and 2017 (Henrickson 2019; Kane 2014). In 2004, the possibility of a consensus became unlikely when it was discovered that 'the GGE failed to even find the smallest common denominator of agreement' over the scope of the introductory GGE and the ability of current international law to regulate the possible hostile uses of ICTs (Henderson 2015). This deliberation was finally put to rest in 2013, when it was established that international law was applicable, but there was no agreement as to how it was applicable. Then, the 2017 GGE was not able to reach a consensus due to the disagreements between participants specifically on the right to self-defense in cyberspace and the previously mentioned applicability of international law, specifically international humanitarian law (IHL), to cyberspace. This topic had already not been included in the 2015 consensus due to objections by the Russian, Cuban, and Chinese delegations. The argument of these nations asserted that the application of IHL in cyberspace would lead to the legitimization of warfare in cyberspace. This led to the selective inclusion of

applicable principles derived from IHL and eventually the lack of consensus at the 2017 GGE (Soesanto et al. 2017; A/70/174). Indeed, this lack of agreement concerning *how* international law applies in cyberspace demonstrates how fragile the agreements on cyber norms really are and how many differences of opinion exist in this realm (Tikk et al. 2018). In the eyes of many, the failure of the 2017 GGE to come to an agreeable consensus spelled the end of this negotiation process, especially when the dissenting delegations pushed for the creation of a 'Working Group of the General Assembly' (Soesanto et al. 2017; Henrickson 2019; Grigsby 2017;).

This failure did not end the GGE process as many expected, since it was then renewed for its sixth round from 2019 to 2021, releasing a long-awaited consensus report in July of 2021 (A/76/135; Schmitt 2021). Instead of focusing on how international law applied to cyberspace, avoiding the conflict that caused an unsatisfactory ending to the 2017 GGE, the 2021 consensus focused on the reaffirmed previously negotiated concepts and elaborated currently established norms to solidify the current understandings of acceptable state behavior in cyberspace. This round of the GGE also focused heavily on confidence building measures, including the establishment of points of contact, dialogue options, and transparency measures (Schmitt 2021).

5.2 OEWG

Voted on in 2018 (with significant overlap of votes for the establishment of another GGE round around the same time) and mandated to begin deliberation in 2019 in conjunction with the new US-supported round of the GGE, the Russian backed Open Ended Working Group was established to study the developments in the field of information and telecommunications in the context of international security and further develop cyber norms. This forum, in comparison to the previous processes, opened up a more inclusive and consultative forum to negotiate cyber norms within the UN (A/73/27; Broeders et al. 2020). This proposal of an inclusive working group for cyber norms was supported by 109 countries out of the 193 member states, indicating that cyber norms are an issue that is attracting increasing attention. Around 150 countries have been involved in this process, producing over 200 documented submissions and 110 hours of deliberations that are now on the record, which is stark change from the lack of interest present

in the early 2000s (Clarke 2021; Basu Et Al 2021). Because of this large pool of participation, some states believe that the OEWG should have the power to "substantively change or rewrite existing cyber norms and agreements". States that do not believe that cyber norms based on current international law are sufficient are using the OEWG to push for expanded and specific norms (Basu et al. 2021). Any member state that has an interest in the current cyber norms negotiations can participate. Non-state actors have also been included in this process, including businesses, NGOs, and academia, through consultative meetings with the OEWG. However, the ultimate decision would still be made by member states, regardless of these consultative meetings' outcome ('UN GGE AND OEWG', Digital Watch 2021; Gavrilovic 202; Gill 2020).

In March 2021, the OEWG came to a consensus that was met with a wide range of reactions. Some believe that the OEWG process has led to a 'stalemate' and has contributed very little to the overall negotiations for cyber norms (Basu et al. 2021). In a process involving so many states, there were concessions that had to be made by all and a stark inability to create any real progress through this report, leading to a feeling of equal disappointment between all parties involved (Ittelson 2021; Stadnik 2021; Basu et al. 2021). Others believe that the OEWG process is a positive step on the road toward establishing cyber norms due to its ability to reaffirm the previous cyber norm consensus among a large contingent of UN member states (Clarke 2021). In the middle, there is the general feeling that this is a good step toward a more concrete consensus in the future. The OEWG has provided new routes of dialogue and inclusivity, and it has renewed a modicum of faith in the process of cyber norm negotiation within UN purview after the failure of the 2017 GGE, which left a six-year gap in the cyber norm consensus (Ittelson 2021; Yoo 2021). Much of the substantive discussion is not included in the consensus document, and instead relegated to the Chairman's summary to be used for future references in cyber norm negotiations (Meyer et al. 2021)

So what does the OEWG consensus say? Overall, the feeling is that it is "new without bringing much new" (Ittelson 2021). A large portion of the final text published at the end of the 2021 OEWG was not included in the consensus document but instead moved to the Chairman's summary (A/AC.290/2021/CRP.3; Stadnik 2021; Ittelson 2021). This, unfortunately, means that a large part of the negotiations and shared views concerning cyber norms are still too contested

to find common ground. Much of the text that ended up being included in the final consensus document have reaffirmed previous negotiations and some of the consensus previously achieved by the UN GGE, but with a wider participation of representatives. Included in the reaffirmed concepts is the idea that the UN charter applies to cyberspace. This includes concepts like state sovereignty and jurisdiction in cyberspace, the need to keep cyberspace "open, secure, stable, accessible, and peaceful", the requirement of states to seek peaceful settlement of disputes, the need to exchange views on cyber norms issues, and the necessity of developing confidence building measures as well as capacity building measures (Ittelson 2021, 2020; Schmitt 2021; Gavrilovic 2020; A/AC.290/2021/CRP.2). The UN OEWG was also able to establish five principles of capacity building, calling for future measures to be

1. a sustainable process, based on mutual trust, driven by nationally identified needs and priorities,
2. comprising specific activities with clear purposes,
3. activities should respect human rights and fundamental freedoms, be gender sensitive and inclusive, be non-discriminatory, and contribute to closing the digital divide,
4. result focused, evidence based, politically neutral, transparent, accountable, and without conditions,
5. undertaken with full respect for the principle of state sovereignty (A/AC.290/2021/CRP.2).

However, there were still numerous points of contention within the OEWG process, focused on the topics of regular institutional dialogue and international law. One of the most highlighted disagreements was if there was a need for a legally binding international instrument specifically designed for issues related to cyberspace. For many, the current international law and previously agreed cyber norms from the GGE process were sufficient to regulate cyberspace on an international level. Others pushed for the creation of an entirely new interpretation of international law specific to cyberspace due to its unique nature. Overall, it was determined that this new framework was not needed, and that the application of international law in cyberspace should be clarified instead (Clarke 2021; Yoo 2021). Additionally, the previous opposition to the inclusion of IHL carried over to the OEWG process, with member states not accepting of 'any draft that contains languages that could justify the use of force in cyberspace' for fear of legitimizing cyber war and the militarization of cyberspace. Ultimately, IHL, the right to self-

defense, accountability measures, and state responsibility were not included in the final consensus document. Instead, these concepts were relegated to either the Chairman's summary or the annex of the consensus document (Yoo 2021; Bau et al. 2021; Clarke 2021; Ittelson 2021). Human rights also took a backseat in the final consensus document (Clarke 2021). Outside of the longstanding contentions present in the cyber norms debate, the OEWG was a platform for those not aligned with the two poles to present their views as well. The focus of these submissions and statements was toward capacity building, state sovereignty in cyberspace, and non-interference in other states' behavior (Clarke 2021).

Of course, the mandate of the OEWG has already been renewed from 2021 to 2025 with essentially the same mandate before the 2019/2021 OEWG even released a consensus document (A/75/240; Meyer et al. 2021). With an extended timeframe to create a consensus in comparison to any of the preceding deliberations and the increased documentation of states' positions on cyber norms thanks to the Chairman's Summary, there is still a possibility of progress in the next few years.

6. Moving Forward with Cyber Norms

Without forward momentum, there is little doubt that the process of creating cyber norms will move outside of the purview of the UN. Certainly, cyber capabilities and threats are developing faster than the process of regulation can keep up with. Additionally, those states participating in cyber norm negotiation lack the flexibility that norms require in order to be a useful tool. If faith were to be lost entirely in the UN process of cyber norms negotiation, this could be ample reason for norm deliberation to move toward other venues. For most states, due to self-interest, this would not be a preferable option. Instead, states must find a way to make progress within UN auspices despite substantial differences of opinion (Broeders et al. 2020; Henderson 2021). The question is, is this progress for the sake of better international cyber regulation or for the dominance of domestic cyber policies internationally?

Now, many are looking toward the proposed Programme of Action (PoA) by France and Egypt supported by forty two states overall. This proposal would establish a regular, annual, and formalized institutional dialogue that would not require renewal to both end the dual track discussions established with the creation of the OEWG alongside the GGE and address the issues arising from cyberspace ("France and Partners Propose a Programme of Action for Advancing Responsible State Behaviour in Cyberspace" 2020). Some believed that the next GGE is likely to be the last because of the transitional track from discussing this proposal in the OEWG to the establishment of the PoA by the UN General Assembly, and were correct in this assumption (Clarke 2021; Yoo 2021; Ittelson 2021). Indeed, the final report of the OEWG stated that the PoA should be elaborated through the next OEWG deliberations, so it is likely to be a key point through 2025. However, there is likely to be significant pushback from states who want to keep the future of cyber norms discussions in the OEWG, ending the dual track discussions in a different way and keeping the primary mode of discussion in the OEWG (A/AC.290/2021/CRP.2; Ittelson 2021).

There is still much to be done to develop useful cyber norms and there is much debate over how this gap should be addressed. Although there seems to be some sort of progress made within these processes despite the challenging differences of opinions between states, there are

calls for a focus on less traditional forms of norm development focused on flexibility and adaptability rather than an international treaty as well as need to ensure adherence to the norms that have already been established. It is unlikely that there will ever be one worldwide 'correct' definition regarding the application of cyber norms. Certainly, with the current political climate surrounding cyber norms and the uncertainty that states have toward solidifying positions on cyber norms, the fact that norms, rules, and principles have been able to emerge is novel itself (Gill 2021; Ruhl et al. 2020; Barrinha et al. 2017; Whitmore et al. 2009). As a relatively new area of norm creation, there is much uncertainty and mistrust between states and their intentions toward cyberspace.

However, it must be noted that the work that has been done on cyber norms has largely been completed backwards. As Finnemore and Hollis (2017) have noted before, norms are developed through a process and are not a 'product' that can just be imposed through UN declaration. Through UN auspices, the beginning of normative statements on the behavior of states in cyberspace have been negotiated and published through the UN, but there is, overall, a lack of adoption of these norms because they have not been socialized in the international community.

7. Primary Analysis Methods

The primary analysis undertaken in this research project examines the time between 2010 and 2021 regarding the progress that promoted Chinese norms have seen at the UN through the GGE and OEWG forums. The next chapter will detail the findings from these analyses, but this chapter will detail the methods with which these primary documents were analyzed. 2010 was chosen as the starting point of this analysis for a few reasons. The first successful forum of the GGE was concluded in this year, so this was a good starting point to track the changes and progress made in developing norms for the internet within the UN. Secondly, 2010 was the year that China published one of its first cyber-related legal texts, the internet White Paper, which set the foundation for future policy in and from China regarding internet governance.

Because this research examines the progress of these promoted norms on the UN level specifically, most documents used in this analysis come directly from UN sources. For the GGE forums, this consists of the final consensus report that is released after the completion of each round. Oftentimes, there are no other UN-based primary documents available from these GGE sessions because of its closed-door format. However, documentation for the OEWG is much more extensive, including working papers, language submissions, and proposals from all states participating in the forum. However, within these documents, the submissions made by the Chinese representative in the UN are prioritized for analysis. The OEWG also published a final consensus report like the GGE forums, which is also included in this analysis.

Of course, there are always normative efforts being made outside of the UN forums, regardless of how much the Chinese government would like the UN to be the center of this cyber norm-making process. However, the spread of norms through bilateral relations, consultations, and other contexts internationally are outside the scope of this research although they are equally as important to research in the future. The UN itself was chosen as the focus for norm negotiation for this research due to the role it plays multilaterally, China's preference for UN forums, and because internationally, this multilateral norm negotiation process is in its early stages. Private companies, organizations, and other internet adjacent norm creating bodies are quite possibly much further in this process, but since the preference of the Chinese government is

to keep internet governance in multilateral hands, this is also outside of the scope of this research.

The main concern of this research is to track the progress of promoted Chinese norms within the UN. In order to do so, a checklist was developed through close reading of documents submitted to the UN by Chinese representatives to establish points of reference. These points were initially extracted from the Chinese Working paper that was submitted to the 2019-2021 OEWG and cross referenced with other documentation submitted to the UN by China relating to internet governance as well as the initial White Paper published by China in 2010. Each point of the checklist used for analysis is justified through accompanying citations from the above listed Chinese policy documents and are included in appendix (A) for further reference. Of the twenty-eight points of reference regarding the norms that China would like to see incorporated, twenty-two can be traced back to documentation from 2010. Out of the remaining six points, four can be traced back to documentation from 2011 and only two remaining points are referenced only in the Working Paper submitted to the 2021 OEWG.

This checklist was then compared with the available consensus documents from each of the successful GGE and OEWG forums. The presence of the reference points gleaned from Chinese-submitted documents is noted with a citation of its paragraph from the five existing consensus documents. In addition, these citations are noted as either explicitly stated or implicitly stated in the final consensus documents with the presence or lack of an asterisk, respectively. This was important to include because the difference between explicitly stated norms and implicitly stated norms is the official inclusion of these norms within the UN versus the possibility for their future inclusion through implicit reference.

Finally, although the checklist itself includes notes on all sections in the consensus documents included in the Working Paper submitted to the UN OEWG (so: threats, norms and principles, international law, confidence building measures, capacity building measures, and institutional dialogue), this analysis will focus specifically on the norms section of the checklist. Because this research project is focusing on norms, it is best to center the analysis around these reference points. In addition, some sections of the checklist repeat concepts that are already

found in the norms section. By focusing on the norms section as most important, repetitive ideas are eliminated as much as possible from the following analysis. However, in moments where reference points from outside of the norms section are relevant, they will be included as needed.

The initial analysis will proceed chronologically, listing the progress made with each specific forum and which of the promoted Chinese norms were included from that year forward in UN internet norms documentation. There are exceptions, especially with the beginning of the OEWG process, where these norms were not carried forward in these documents and will be noted accordingly. Finally, the preferred Chinese norms that have not so far been included in codification on the UN level and their level of importance to China's normative platform overall will be discussed.

8. Initial Analysis

Although this analysis begins in 2010, there was not much progress made in developing norms through the UN during this first successful round. The focus of this forum was establishing an understanding of what threats the internet poses to states. The consensus document published by the 2010 GGE forum included explicit mention of half the applicable threats that were listed as reference points in the checklist, with only one being not fully explicit (A/65/201). In addition, fake news as a threat was not quite applicable to the 2010 GGE forum because of its rise to prominence in the latter half of the 2010s. Overall, the inclusion of the reference points in the threats section within this and future consensus documents has remained largely the same with only small variations. This continuity over the last decade has led to an overall agreement between states on what threats the internet faces. However, this does also mean that this established agreement may be missing key issues that have developed since 2010. China also was not focusing heavily on promoting the domestic policies developed for internet regulation internationally yet. In fact, the first Chinese-published white paper on the internet was not publicized until mid-2010, when the first UN GGE forum would have been largely complete already.

8.1 2013 GGE

Figure 1: 2013 GGE China-Preferred Norm Development Summary (A/68/98)

- State sovereignty and jurisdiction over cyberspace (clause 20)
- Disallow malicious use of ICT by the state or other actors (clause 19, 23)
- Restriction of terrorist/criminal group access to the internet (clause 22)
- Increase cooperation between intelligence and law enforcement (clause 22)
- Continue negotiations on cyber norms within UN auspices (clause 13)

In 2013, the beginnings of the norms present within UN processes regarding internet regulation internationally took shape. This iteration of the GGE is most well-known for establishing that international law is applicable within the cyber realm, but also started the discussion of which specific norms would need to be codified (A/68/98, clause 16). For China-specific norms, this

codification included references or justification for about one-third of the PRC's preferred norms, but only half of those were explicitly stated within the final consensus document. Most importantly, this consensus document established that "state sovereignty and international norms and principles that flow from sovereignty apply to the state conduct of ICT related activities, and to their jurisdiction over ICT infrastructure within their territory" (see Figure 1).

Since the introduction of the internet to the country, China has been an advocate for extensive systems of security related to its internet systems, known as the Golden Shield Project. In use since 2008, this project encompasses several initiatives, but the most well-known is the so-called Great Firewall of China (Chandel et al. 2019). These internet security systems allow the government of China to enforce domestic law and state jurisdiction over the internet systems present within the borders of China. This, at its core, is what China calls cyber sovereignty the main tenant of China's preferred cyber norms. This concept relies on the idea of sovereignty and the state's right to control its territory, make its own laws, and remain free from the interference of other states into domestic affairs. By extension, the assertion of state sovereignty over the internet also includes the normative concept of disallowing foreign state interference using ICT technology.

For cyber sovereignty to become internationally recognized, the sovereignty of the state over the internet must also be recognized. This concept was recognized in the 2013 GGE consensus report, marking a possible major step forward for the codification of cyber sovereignty at the UN level. This was the first step towards normalizing the idea of cyber sovereignty, but it was certainly one of the easier norms to be agreed upon. Since sovereignty of the state holds precedent, recognized internationally, and enshrined in the UN charter, it would be one of the easier norms to find common ground on. After all, in a multilateral forum, the first concept to establish is if the state has the right to regulate or legislate over the cyber realm. By declaring the internet as part of sovereign state territory, multilateral forums such as the UN can work toward more concrete regulation with less legitimacy issues. However, the final consensus document also includes the statement that "efforts to address the security of ICTs must go hand in hand with respect for human rights and fundamental freedoms" (A/68/98). This inclusion, in theory, does undercut the idea of absolute state sovereignty over the internet.

Also included in the 2013 consensus report was the condemnation of the malicious use of ICT by states and other actors (see Figure 1). The text itself includes that "states must meet their international obligations… must not use proxies… seek to ensure that their territories are not used by non-state actors for unlawful use of ICTs" (A/68/98). This statement, however, leaves quite a bit of wiggle room. It is deliberately ambiguous, referring to the vague 'international obligations' of states. This phrase could be interpreted in many ways and does very little to dissuade or curtail states themselves from engaging in malicious ICT activity. The idea of preserving the peace and stability of the international community is certainly present in the idea of 'international obligations', but the differing interpretations of what constitutes peace and stability leave a large gray area. Even today, there is very little agreement on what the obligations of the state are in cyberspace and interpretations vary widely. However, it does create some specificity for actors outside of the state as well as establishing state responsibility for at least monitoring ICT usage within their territory. Both proxies and non-state actors are mentioned in this statement, seemingly disallowing the malicious use of ICTs by any actor other than the state.

This theme is also continued in reference point 33, which focuses on the restriction of terrorist internet use for recruitment or content proliferation. It is encouraged in the final consensus report that "states should intensify cooperation against criminal or terrorist use of ICTs" (A/68/98). Although this does not explicitly ban the presence of criminal or terrorist content on the internet, it certainly encourages states to shut down access that these groups may have to the internet. Certainly, this sort of wording focuses more on the access that malicious non-state actors may have to the internet but does not specifically focus on the content that these actors produce. The normative phrasing that China submitted with its working paper focuses much more on the content rather than access, making this not quite an explicit match, but close in concept.

Cooperation and exchanges of intelligence and law enforcement emerged as an encouraged norm in the 2013 consensus document as well, following the trend of assent towards information sharing. The idea of sharing information regarding all aspects of state practices has a

history within the creation of cyber norms. Indeed, before even the first GGE, the UN chairman of the time asked for submissions detailing state policy opinions regarding cyberspace and received very little. The encouragement for sharing information is a UN staple to promote transparency and understanding between states. It is not surprising that the first promotion of information sharing in this GGE consensus report concerns intelligence and law enforcement due to its mandate being security focused. This certainly aligns with the priorities of preferred Chinese norms, which have a focus on eliminating all content from criminal or terrorist organizations. The question is then, will future reports on cyber norms then define what a terrorist or a criminal organization is in terms of non-state actors who have access to ICT? Or will it remain up to each state to determine what constitutes terrorist or criminal activity?

Given the reliance that most states have on ICT infrastructure and the internet, it is not surprising either that one of the Chinese preferred norms mentioned in the 2013 consensus document is to secure the supply chain of ICT-related goods. However, this mention is not in the normative section as would be expected. During this time in the negotiations for cyber norms, supply chain security was included in the threats section rather than with the normative considerations. This is certainly a good start.

Finally, China's preference for continuing the negotiations of cyber norms within the UN is confirmed. As mentioned previously, China would rather these negotiations take place at the UN instead of the currently common multistakeholder model. This preference for multilateral participation with only nominal contributions from non-state entities is reflected in consensus documents from the GGE moving forward. It is the forum's hope that "the UN should play a leading role in promoting dialogue among member states to develop common understandings". Certainly, the forum has an interest in keeping these discussions active at the UN level because without them, it will be much more complicated to develop common understandings between states. These common understandings then generally develop into norms, but in this case this process is hardly organic.

8.2 2015 GGE

Figure 2: 2015 GGE China-Preferred Norm Development Summary (A/70/174)

- Critical Infrastructure and Critical Information Infrastructure protection (clause 13f)
- Disallow the undermining of CI/CII of a state by other states (clause 13f)
- Protection of CI/CII is the states' responsibility (clause 13g)
- Prevent the use/proliferation of harmful hidden functions (clause 13i)
- Report vulnerabilities within ICT (clause 13j)
- Secure the supply chain of ICT and related goods (clause 13i)
- Further work needed on cyber norms (clause 9, 15)

The 2015 GGE has been the most productive forum for the creation of cyber norms at the UN so far. It was this consensus document that established the thirteen cyber norms, listed in Figure 3, that were later adopted by the General Assembly without a vote. In the UN, if even one state does not agree with the resolution, then there must be a vote called to measure the response to the proposed resolution. However, in this case, since there was no vote, it is significant that all states agreed with the codification of the document. Of course, the established norms are non-binding and entirely voluntary, and part of this consensus may have been caused by this. It is also this consensus report that explicitly includes just over a third of China's preferred cyber norms. Since this document, there has arguably not been any significant progress on UN-developed cyber norms, seeing as the 2021 GGE solely expanded on these already established norms.

This consensus document was the first to recognize the importance of protecting CII/CI and explicitly mentions that states are expected to "not knowingly support ICT activity… that intentionally damages critical infrastructure" (See Figure 2). However, what is not included here is a definition of what CI/CII is. For some states, this includes mostly public services that are imperative to daily life. These often include electricity grids, water systems, transportation systems and other such infrastructures. The Chinese definition of critical infrastructure is much broader. The first tentative Chinese definition of CI/CII can be found in the 2017 Chinese Cybersecurity Law and includes the following; "public communication and information services,

power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which - if destroyed, suffering a loss of function, or experiencing leakage of data - might seriously endanger national security, national welfare, the people's livelihood, or the public interest" (The Standing Committee of the People's Congress, 2016). While the first half of this definition is fairly standard in covering what states generally consider to be part of CI/CII, the latter half then allows for almost any online service or platform to be considered a part of CI/CII if certain conditions are met.

Indeed, the Chinese definition of national security alone is broad and encompassing. The 2015 National Security Law of the People's Republic of China defines national security as "the relative absence of international or domestic threats to the state's power to govern, sovereignty, unity, and territorial integrity, the welfare of the people, sustainable economic and social development, and other major national interests, and the ability to ensure a continued state of security". The broad nature of this definition alone allows for many infrastructures to be included as CI/CII, expanding the area of what should not normatively be interfered with through ICT.

Less explicitly stated in the 2015 consensus document is the normative concept of refraining from using policy or technological advantage to undermine the CI of other states (See Figure 2). The inclusion of no state interference from the 2013 consensus document as well as the newly included norm of cyberattacks on CI/CII being off limits, it can be interpreted that a state using an advantage they have to interfere with another state's CI/CII would qualify as unacceptable state behavior. Protecting CI/CII should be the focus of state effort on this subject. Indeed, the 2015 consensus document includes a few reference points from China's preferred cyber norms in this direction. The first is the encouragement for "states [to] consider how best to cooperate to exchange information" (A/70/174). Much like in the 2013 consensus document where legal regulatory bodies were encouraged to share information, this preference for information sharing and transparency has now been expanded to the 2015 consensus document in a more general sense. However, the preferred Chinese norm refers specifically to sharing information relating to protecting CI/CII. Considering the prominence that CI/CII holds in the previously discussed norm, it is safe to say that even if not specifically mentioned, CI/CII-related information sharing is included in the more general statement of the 2015 consensus report.

Additionally, this report established that the protection of CI/CII from outside ICT threats was the state's responsibility. The reference point related to this inclusion asserts that the state should take full responsibility to protect its ICT systems through legislation, including all ICT systems as well as critical data, and not just CI/CII. But, as mentioned before, the broad definition of CI/CII held by the Chinese government would allow for much to be considered within this category, making this preferred norm present but not quite explicitly stated. Three reference points relating to the illegal attainment of data can also be extrapolated from the 2015 consensus document. The first is the norm of banning the use of ICT-enabled espionage by states against states resulting in the theft of important data or mass surveillance or any illegal attainment of data. Considering that in 13c and 13f it is stated that 'states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs" and that "a state should not conduct or knowingly support ICT activity… that intentionally damages critical infrastructure", it can be interpreted that the theft of data that is a part of the broad understanding of CI/CII is prohibited. The lack of specificity in these two clauses opens up the possibilities of what could be seen as unacceptable state behavior.

Data itself is increasingly important to ICT systems worldwide and this is no exception in China. Indeed, regardless of the importance of the data, the 2017 Cybersecurity Law also establishes that the attainment of data through any illegal means is forbidden. These illegal means are also covered within 13i of the consensus report, which includes that "states should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions" (A/70/174). These functions, tools, and techniques are often used to acquire data, which support the Chinese normative idea of forbidding the use of these strategies, including backdoors. In addition, it is included explicitly in both the preferred Chinese norms as well as the 2015 consensus report that if these strategies are found including other vulnerabilities not specifically listed, that "states should encourage responsible reporting of ICT vulnerabilities and share associated information" (A/70/174).

In the 2015 consensus document, it is also explicitly stated that the security of the supply chain should be guaranteed (See Figure 2). In the previous 2013 document, supply chain security

was only mentioned within the threats section of the published consensus report. Now, however, it is included with published 2015 norms in 13i: "states should take reasonable steps to ensure the integrity of the supply chain" (A/70/174). This explicit statement supporting the security and integrity of the supply chain also supports the interpretations and arguments for two other reference points, including the prohibition of limiting market access to ICT based on national security concerns and of blocking independent state control of ICT goods, services, and security. If the state is responsible for the security of ICT as argued previously, then they should be able to secure access to the needed goods and services to build up their ICT and related security without interference from others. The idea that national security concerns could prevent or stop the supply chain from reaching a specific nation could be seen as hurting the integrity of the supply chain; ICT is a necessity to most infrastructures in society and by denying access, these infrastructures are compromised.

Additionally, the encouragement from the previous 2013 consensus report of information sharing between regulatory bodies has now expanded in the 2015 consensus report. Whereas before, the wording was "states should intensify cooperation… between respective law enforcement and prosecutorial agencies", this has changed to "states should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs…" (A/68/98; A/70/174). Previously, this sentiment was limited to a narrow view of legal bodies responsible for pursuing crime. Now, however, this definition of cooperation has expanded far beyond the purview of just legal bodies. It is encouraged that all relevant bodies within the state work with other states to solve the issues of cybercrime and terrorism. Although this does not specifically mention international organizations, Chinese staff within international organizations such as the UN are almost always government employees. This, and China's preference for working on internet governance within multilateral forums makes this preferred norm present, but not necessarily explicit.

Finally, the 2015 consensus document makes the first reference to the need to further study the norms, rules, and principles that should apply to cyberspace. Considering that this consensus document contained the first codification of UN norms regarding cyberspace, this is a recognition from both China and the other participating states on the GGE that there must be

more progress made on cyber norms. This list, while still being a very general list that was non-binding and voluntary, was only the beginning of the issues that might need defined state behavioral guidelines.

Figure 3: 2015 GGE est. Cyber Norms as adopted by UNGA (A/RES/73/27, clauses 1.1-1.13)

States should;
- cooperate to stabilize and secure ICT
- consider all relevant information regarding ICT incident attribution
- not knowingly use territory for malicious ICT acts
- consider widespread cooperation to address ICT threats
- recognize human rights specific to the internet
- not support actions that harm CI/CII
- take measures to protect their CI/CII
- respond to requests from states whose CI/CII has been damaged
- take measures to secure the supply chain of ICT products
- prevent use of malicious ICT tools and hidden functions
- encourage responsible reporting of ICT vulnerabilities
- not take actions that will harm cyber emergency response teams
- cooperate with civil society and the private sector to improve ICT security

8.3 2021 OEWG

Figure 4: 2021 OEWG China-Preferred Norm Development Summary

- State sovereignty and jurisdiction over cyberspace (lost norm)
- Increase cooperation internationally between intelligence and legal units (lost norm)

Although the 2021 GGE and OEWG were held at roughly the same time, held very similar mandates, and were supposed to be working forward from the 2015 consensus document, the two groups published very different consensus documentation. For the GGE, the 2021 consensus document was truly an expansion on the previous norms established in the 2015 round. Extra explanation and possible scenarios were included in reference to expand the scope of previously established UN norms. However, the OEWG chose to take the previous work of the GGE and

use it as a guide for those states that were new to the process. In fact, there are very many points between the 2015 GGE that did not carry over into the 2021 OEWG document. In the past GGE forums, negotiated points carried through and built upon each other to reach normative understandings. This was not the case in the OEWG, and although there were statements reaffirming the normative document voted in by the General Assembly, much of that material was left unrecognized. This could be for several reasons. State assertion in their documentation that previous negotiation was null and void because they were not involved in its creation, the newly open membership format, and carry over issues from the previously failed 2017 GGE could all have played a role.

The most significant of these is state sovereignty and jurisdiction over cyberspace within a states' territory (See Figure 1 and 4). In the 2013, 2015, and 2021 GGE document, the right of the state to sovereignty over "the state conduct of ICT related activities, and to their jurisdiction over ICT infrastructure within their territory" is explicitly included in each consensus document (A/68/98; A/70/174). In all three, this is explicitly stated as well as being one of the preferred norms that China promoted in its policy documents as well. However, the right to state sovereignty and jurisdiction is not mentioned explicitly at all in the OEWG consensus document. The only reference to this concept is within international law, where the Charter of the United Nations, which includes state sovereignty, is reaffirmed. This is quite the step back in comparison, resulting in the loss of an explicitly stated preferred norm from UN cyber norms documentation.

Although it did carry through to the 2021 GGE, this is concerning for the progression of cyber norms as it seems to be the OEWG that is the currently preferred forum within the UN. The norm of state sovereignty in cyberspace is, as was previously explained, the cornerstone to the three key norms out of China's submitted list. Without the establishment of state sovereignty over ICT, this also means that the loosely established responsibility of the state for ICT and critical data protection was also scrapped. How can you assert responsibility without having confirmed control over the areas the state is responsible for?

Also lost from this document is the encouragement for states to cooperate and exchange information and assistance in regard to legal prosecution of criminal activities online (See Figure 1 and 4). Many concepts and normative understandings that had been developed over the GGE process were lost with the 2021 OEWG document, resulting in a consensus report that reflects the negotiations previously pursued in the 2013 GGE forum. In fact, the percentage of explicit mentions of preferred Chinese norms is only increased by one reference point between the 2021 OEWG and the 2013 GGE. Moving forward, it will be interesting to see the progress that the OEWG makes in its 2021-2025 iteration.

8.4 2021 GGE [5]

Figure 6: 2021 GGE China-Preferred Norm Development Summary (A/76/135)

- ICT infrastructure and critical data protection are the state's responsibility (clause 44, 47)
- No illegal attainment of data (clause 58)
- No backdoors (clause 58)
- Cooperate with international organizations to counter terrorism (clause 31)

The 2021 GGE, while not necessarily creating new norms for cyberspace, did clarify some aspects of the previously established norms through extended explanation and recommendations for implementation. For the promotion of Chinese norms, this meant that some previously not explicit preferred norms became officially included in the UN cyber norm documentation. For example, included in the 2021 expansion of the 2015 norms is the explicit confirmation that, indeed, ICT infrastructure and critical data protection are within the responsibilities of the state (See Figure 2 and 6). In addition, this clarification in clause 44 states that "each State determines which infrastructures or sectors it deems critical within its jurisdiction, in accordance with national priorities…" (A/76/135). This addition leaves the work of defining critical infrastructure to the state. In theory, this means that states can determine that much of the internet falls under their jurisdiction, much like China has already done.

[5] Please see Figure 7 in Appendix B for a highlighted summary of the 2021 GGE consensus document. Due to its length, this figure was moved out of the main body of the text.

This consensus document also makes it explicit that "state practices such as arbitrary or unlawful mass surveillance may have particularly negative impacts on the exercise and enjoyment of human rights" (A/76/135). Whereas before, the condemnation of mass surveillance was couched in the norm protecting human rights online, now it has been made explicit. The safeguards that should be included with ICT products and data were also greatly expanded, including the condemnation of backdoors, recommendations for safety procedures, and encouragement to create legislation to enhance the protection of data. An increase of legislation and safety measures means that now, previously undefinable situations can be brought under the legislative jurisdiction of the state, who will then determine what constitutes an illegal access of data or otherwise harm to the ICT infrastructure or critical data of the nation. Of course, the meaningfulness of these inclusions depends on how much of the 2021 GGE consensus document future OEWG forums are willing to include in their own consensus documents.

The only reference point listed within China's preferred norms that did not carry over from the previous GGE forums and the OEWG process is the need for further study on the norms, rules, and principles of cyberspace. However, this point is not included in the 2021 GGE forum, which is most likely because of the choice to not renew the GGE process. Instead, the OEWG process was renewed in December 2020 with a mandate from 2021 to 2025 (A/RES/75/240). Because the UN chose to renew the OEWG over the GGE before it had even been determined to be successful, it is possible that the representatives of the 2021 GGE chose not to include the need for further study in their consensus report because the OEWG was being prioritized over the continuation of the GGE.

8.5 What has not been included?

It is also important to talk about what has not been included in this context. As much progress as China has made in including its preferred norms in UN norm negotiation, there are still important points that the legitimation of Chinese norms hinge on. Specifically, this is referring to point 12, the state's right to enact ICT-related legislation consistent with national circumstances, and point 13, that the availability of information on the internet should be based on national laws and regulations based on the considerations of national security and public order. Along with

reference point eleven, that states have jurisdiction and sovereignty over ICT infrastructure, resources, and activity, these three norms are the most important to China's normative strategy internationally. However, only point eleven has been included in any consensus report documentation. The inclusion of this norm is supported by the UN charter, which explicitly mentions state sovereignty and territoriality, leading to the fairly obvious interpretation of state sovereignty over ICT. The exclusion of points twelve and thirteen are equally important to examine as well. These two preferred norms include that the state has a right to make ICT policy consistent with national circumstances and that information available on the internet should be regulated by relevant national laws and regulations. Because there has been no progress made with these two norms, the legitimation strategy that China is pursuing through the promotion of their version of internet norms has not made much progress.

9. Discussion

On the surface, it seems that Chinese cyber norm promotion has made some progress within UN forums. Without nuance, it would seem that the progress of Chinese norms within the UN would lie somewhere between the emergent stage and the cascade stage of Finnemore and Sikkink's norm life cycle. With a 36% jump from 2010 to 2021 of explicitly stated norms being included in UN documentation, it certainly seems that there has been significant progress for China in a nascent negotiation process. This increasing inclusion of China's preferred norms in UN cyber norms documentation could easily lead to the belief that the other states will soon be adopting these preferred norms. However, three things are currently weighing down the success of Chinese norm promotion.

The first is the switch away from the GGE to the OEWG forum. This decision, while opening up the field of negotiation to the rest of the states with membership in the UN, has significantly set back the timeline of meaningful progress of UN cyber norm creation. The OEWG, while established with the intention to move the cyber norms negotiation outside of the GGE, was not able to find consensus between all participants. Concepts that had been previously agreed upon were discarded and questioned, documentation that had already been unanimously adopted was challenged, and the resulting consensus document read like an almost decade old consensus report. By switching the forum to the OEWG, the semi-linear progress made by the GGE on cyber norms has now doubled back on itself. In the short term, this would be considered a negative development.

Since technological development moves much faster than the UN, the lack of progress on cyber norms within UN auspices gives rise to questions about the worth of these forums in the cyber norm debate. However, in the long term, this disagreement just shows how many of the assumed "established" cyber normative concepts were not multilaterally accepted, let alone established. By excluding the majority of states from this negotiation process, there has been a false sense of progress among those working on cyber norms. By all means, the inclusion of other nations within this negotiation process is a much more transparent choice, but without significant progress in a new forum, the UN may find itself far outside of the cyber norm

negotiation process. By extension, China's main platform for the promotion of its cyber norms would be made irrelevant, which is hardly the preferred outcome.

Secondly, the lack of progress regarding the inclusion of two of China's three most important cyber norms does not bode well for true adoption of Chinese cyber norms. The first, state sovereignty and jurisdiction over the ICT infrastructure, resources, and activities within its territory, has been tentatively established, even if it was not listed in the consensus report of the OEWG. It is possible that the normative concept of sovereignty in cyberspace was established in part by Chinese efforts, but it is more likely that this victory stems from the foundations of the UN Charter. The second and third, however, have not been included explicitly or through interpretation in UN documentation. This refers to the norm of the state's right to make ICT policy consistent with national circumstances and of information being made available on the internet based on the relevant laws and regulations of that state. In order for Chinese norm promotion to be successful, all three must be normalized within international society.

Where the establishment of state sovereignty over cyberspace forms the base of China's argument for cyber sovereignty, it does not give allowance to the actions that China takes to regulate the internet. Based on the UN documentation, this state sovereignty should be limited by the human rights of domestic citizens. Considering that a large part of Chinese domestic internet policy is to create a "healthy internet ecosystem", as defined by the state, the normalization of content regulation in accordance with the national circumstances as defined by the state is a necessary part. The closest that the consensus documents from this process have gotten to either of these norms is found in the 2021 GGE consensus document. In clause 44, it is stated that "each state determines which infrastructures or sectors it deems critical… in accordance with national priorities" (A/73/135). This clarification of the norm related to critical infrastructure protection sounds similar to the idea that states have the right to make ICT policy according to the national circumstances. It is possible that this clarification may be able to set the foundation for this norm to be included in the future.

Finally, the nuance needed to support the internalization of Chinese preferred cyber norms is not present within these consensus documents. It is true that over a third of the

analytical checklist has been explicitly included, but the included points are not very controversial. In fact, most of the agreed-upon points can be tied back to the UN Charter. The very first article of the Charter concerns the maintenance of "international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace" (UN Charter 1945). This principle is central to six of the fourteen explicit norms stated in the 2021 GGE consensus report. The eight other explicit norms not included in the previous statement can also be compartmentalized based on the Charter. Article 1 includes the notion of achieving "international co-operation in solving international problems of an economic, social, cultural, or humanitarian character", which covers four reference points related to information sharing and intranational cooperation. Lastly, Article 2 established state sovereignty and non-interference within another state, giving precedence for the last explicit points as well (UN Charter 1945).

This lack of nuance specific to Chinese efforts in the United Nations' cyber norms process and the overwhelming presence of the UN Charter in the consensus already found indicates that Chinese cyber norm promotion still needs much more work to reach internalization. In reality, with these considerations taken into account, it would be much more accurate to say that Chinese preferred norms are stalled in the first stage of the norm life cycle in regard to the UN. Their norms have been introduced and are known by other states, but are not being widely adopted because of China's actions as a norm entrepreneur. The progress that has seemingly been made is due to outside factors, negating the idea of China's preferred norms cascading through UN policies.

10. Conclusion

The core aim of this research project is to assess the progress of Chinese-promoted cyber norms within United Nations cyber norm negotiation processes from 2010 to 2021. As a challenger for the United States dominated cyber norms, China hopes to introduce its own norms internationally, to find acceptance for these norms, and to have these norms internalized by other states. The data taken from consensus documents detailing the cyber norm negotiation process, without contextualization, seems to indicate that these norms are finding acceptance within the UN by other states.

However, when the various political and institutional factors are taken into consideration, this initial assumption can be rejected. This research finds that Chinese efforts at the UN to influence the standards of state behavior on the internet have not come to fruition quite yet. This is due to the absence of specific norms key to China's norm "package" from UN documentation, specific additions to UN documentation regarding human rights, and the lack of nuance to support specifically China's promoted norms within these documents.

Based on Finnemore and Sikkink's life cycle, China's cyber norm "package" would still be firmly within the first stage of emergence, considering the lack of consensus regarding these norms. In addition, it is very unlikely that the second stage, a norm "cascade", will happen any time soon for China, especially when one considers that most of China's successfully promoted norms have found acceptance through sources that are not linked to China's efforts. Most of China's successful cyber norms coincide with principles found in the UN Charter, established far before Chinese cyber norms, and there is little support for other key, not already accepted Chinese cyber norms by other states. Indeed, most UN consensus documentation for cyber norms cite human rights and freedoms prominently, making it all the more unlikely that other states would consent to add the necessary clauses that would lead to the internalization of Chinese cyber norms internationally. It is much more likely that the promotion of Chinese norms internationally will stall within the emergence stage of the norm life cycle and these norms are not likely to be adopted, let alone internalized.

This is especially true due to the move of cyber negotiations from the GGE to the OEWG. As demonstrated in this research, the OEWG took a serious step back from the norms that were already established within the GGE. The exclusion of cyber sovereignty, China's most well-known cyber norm, from the final OEWG consensus document indicates the lack of stability present in the cyber negotiation process. The inclusion that the OEWG embodies in the cyber norm negotiation process is both a blessing and a curse for Chinese-promoted cyber norms. With a larger audience to potentially adopt these norms also comes differing perspectives that may negatively impact the acceptance China's cyber norms may find.

But is the negotiation of cyber norms through normative packages derived from domestic policy the best route to take in establishing multilateral cyber governance? Throughout this thesis, it has been noted that much of the processes and rationale behind the current cyber norm negotiation are inflexible and inadequate. Regardless, the analysis given must reflect the reality of how states are approaching this issue, requiring the measure of normative success to rely on these packages. Certainly, Finnemore and Sikkink's critique of cyber norm packages promoted by different states supports the idea that there needs to be a more contentious effort by states to adopt international norms that fit the current scenario, rather than norms that support the national priorities of states. Indeed, the measurement of normative success would change if the documentation relevant would be analyzed for practicality and real-world applicability. The promotion of norm packages has helped to drive the cyber norm negotiation process to the stalemate that has largely been present since the failure of the 2017 GGE process and loss of progress in the 2021 OEWG.

By far, it would be better if these forums aimed for flexibility, adaptability, and practicality in their norm negotiation. Presenting norms as packages, where many must be accepted into final documentation in order to find success as a norm entrepreneur, is detrimental to the creation of useful cyber norms. In addition, the development of technology far outstrips the pace that states can attempt to regulate cyberspace internationally and will continue to fall behind if this negotiation process does not change. States would be better served in the cyber norm process to consider how their promoted norms match the international cyber reality and act accordingly.

References

"Administrator of Domain Name System Launches Global Multistakeholder Accountability Process." ICANN Announcements. ICANN, March 14, 2014. https://www.icann.org/en/announcements/details/release-administrator-of-domain-name-system-launches-global-multistakeholder-accountability-process-14-3-2014-en.

"China's Submissions to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications Inthe Context of International Security." Open Ended Working Group. UNODA, 2019. https://front.un-arm.org/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.

"Developments in the Field of Information and Telecommunications in the Context of International Security – UNODA." Developments in the field of information and telecommunications in the context of international security. United Nations Office of Disarmament Affairs. Accessed March 2, 2022. https://www.un.org/disarmament/ict-security/.

"Digital around the World - Datareportal – Global Digital Insights." DataReportal, 2021. https://datareportal.com/global-digital-overview#:~:text=A%20total%20of%205%20billion,12%20months%20to%20April%202022.

"FACT SHEET; DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY." UNODA. United Nations, July 2019. https://front.un-arm.org/wp-content/uploads/2021/07/ICT-Security-Fact-Sheet-July2021.pdf.

"Full Text: White Paper on the internet in China." China Daily, June 10, 2010. https://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm.

"International Strategy for Cyberspace - Whitehouse.gov." White House Archives. The White House, May 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

"National Security Law (2015) 国家安全法 -." China Law Translate, September 11, 2020. https://www.chinalawtranslate.com/en/2015nsl/.

"United Nations Charter." United Nations. United Nations, 1945. https://www.un.org/en/about-us/un-charter/full-text.

"UN E-Government Knowledge Base; Data Tables 2020." New York, New York: 2021.

"UN GGE AND OEWG." Digital Watch. Geneva internet Platform, February 4, 2022. https://dig.watch/processes/un-gge.
119-184

Adamson, Liisi, Dennis Broeders, and Bibi van den Berg. “International Law and International Cyber Norms: A Continuum?” Chapter. In Governing Cyberspace: Behavior, Power, and Diplomacy, 19-43. London: Rowman & Littlefield, 2020.

Almeida, Virgilio A.F. “The Evolution of Internet Governance: Lessons Learned from Netmundial.” IEEE Internet Computing 18, no. 5 (2014): 65–69. https://doi.org/10.1109/mic.2014.98.

Ambos, Kai. “International Criminal Responsibility in Cyberspace.” Research Handbook on International Law and Cyberspace, 2015, 118–44. https://doi.org/10.4337/9781782547396.00015.

Arsène, Séverine. “Global internet Governance in Chinese Academic Literature.” China Perspectives 2016, no. 2 (2016): 25–35. https://doi.org/10.4000/chinaperspectives.6973.

Barlow, John Perry. “A Declaration of the Independence of Cyberspace.” Electronic Frontier Foundation, April 8, 2018. Originally published 1996. https://www.eff.org/cyberspace-independence.

Barrinha, André, and Thomas Renard. “Cyber-Diplomacy: The Making of an International Society in the Digital Age.” Global Affairs 3, no. 4-5 (2017): 353–64. https://doi.org/10.1080/23340460.2017.1414924.

Basu, Arindrajit, Irene Poetranto, and Justin Lau. “The UN Struggles to Make Progress on Securing Cyberspace.” Carnegie Endowment for International Peace, May 19, 2021. https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491.

Bloomfield, Alan. "Norm Antipreneurs and Theorising Resistance to Normative Change." Review of International Studies 42, no. 2 (2016): 310-33. doi:10.1017/S026021051500025X.

Boudon, Raymond. “Beyond Rational Choice Theory.” Annual Review of Sociology 29, no. 1 (August 2003): 1–21. https://doi.org/10.1146/annurev.soc.29.010202.100213.

Broeders, Dennis, and Berg Bibi van den. Governing Cyberspace Behavior, Power, and Diplomacy. Lanham: Rowman & Littlefield, 2020.

Broeders, Dennis, and Fabiano Cristiano. “Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road.” ISPI, April 2, 2020. https://www.ispionline.it/en/pubblicazione/cyber-norms-and-united-nations-between-strategic-ambiguity-and-rules-road-25417.

Broeders, Dennis, Berg Bibi van den, Dennis Broeders, and Bibi van den Berg. “Governing Cyberspace: Behavior, Power and Diplomacy.” Essay. In Governing Cyberspace: Behavior, Power, and Diplomacy, 1–18. London: Rowman & Littlefield, 2020.

Buchan, Russell. “Cyber Espionage and International Human Rights Law.” Research handbook on international law and cyberspace, 2019, 168–89. https://doi.org/10.5040/9781782257370.ch-005.

Budnitsky, Stanislav, and Lianrui Jia. “Branding internet Sovereignty: Digital Media and The CHINESE–RUSSIAN CYBERALLIANCE.” European Journal of Cultural Studies 21, no. 5 (2018): 594–613. https://doi.org/10.1177/1367549417751151.

Burnay, Matthieu, and Julien Chaisse. “Global Commons as an Emerging Arena Of CONTESTATION of Global Governance Structures and Norms.” International Community Law Review 22, no. 5 (2020): 533–58. https://doi.org/10.1163/18719732-12341446.

Cai, Congyan. "The Rise of China and the Strategy of Universality of International Law." China International Strategy Review, 2021, China International Strategy Review, 2021-05-17.

Calderaro, Andrea, and Anthony J. Craig. “Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building.” Third World Quarterly 41, no. 6 (2020): 917–38. https://doi.org/10.1080/01436597.2020.1729729.

Carr, Madeline, and Feja Lesniewska. “internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance.” International Relations 34, no. 3 (2020): 391–412. https://doi.org/10.1177/0047117820948247.

Cheek, Timothy. “Xi JINPING’S Counter-Reformation: The Reassertion of Ideological Governance in Historical Perspective.” Journal of Contemporary China, 2021, 1–13. https://doi.org/10.1080/10670564.2021.1893554.

Chircop, Luke. “TERRITORIAL SOVEREIGNTY IN CYBERSPACE AFTER TALLINN MANUAL 2.0.” Melbourne Journal of International Law 20 (2019): 1–29.

Cho, Yoonyoung, and Jongpil Chung. “Bring the State Back in: Conflict and Cooperation among states in Cybersecurity.” Pacific Focus 32, no. 2 (2017): 290–314. https://doi.org/10.1111/pafo.12096.

Clarke, Laurie. “UN Cybersecurity AGREEMENT: Historic but Likely Ineffective.” Tech Monitor. New statesman, April 22, 2021. https://techmonitor.ai/policy/geopolitics/un-countries-cybersecurity-deal-state-sponsored-attacks.
Congressional Research Service. “Defense Primer: Cyberspace Operations.” Project on Government Secrecy. Federation of American Scientists, 2021. https://sgp.fas.org/crs/natsec/IF10537.pdf.

Couture, Stephane, and Sophie Toupin. “What Does the Notion of ‘Sovereignty’ Mean When Referring to the Digital?” New Media & Society 21, no. 10 (2019): 2305–22. https://doi.org/10.1177/1461444819865984.

Creemers, Rogier, Dennis Broeders, and Berg Bibi van den.. “China’s Conception of Cyber Sovereignty: Rhetoric and Realization.” Chapter. In Governing Cyberspace Behavior, Power, and Diplomacy. Lanham: Rowman & Littlefield, 2020.

Creemers, Rogier, Graham Webster, Paul Triolo, Katharin Tai, Lorand Laskai, and Abigail Coplin. “Lexicon: 网络强国 Wǎngluò Qiángguó.” Cybersecurity Initiative. New America, May 31, 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo/.

Creemers, Rogier, Mingli Shi, Lauren Dudley, and Graham Webster. “China's Draft 'Personal Information PROTECTION Law' (Full Translation).” China's Draft 'Personal Information Protection Law' (Full Translation). New America, October 21, 2020. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/.

Creemers, Rogier, Paul Triolo, and Graham Webster. “Translation: Cybersecurity Law of the People's Republic of China (EFFECTIVE June 1, 2017).” Cybersecurity Initiative. New America, June 29, 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

Creemers, Rogier, Samm Sacks, and Graham Webster. “Translation: Critical Information Infrastructure Security Protection REGULATIONS (Effective Sept. 1, 2021).” DigiChina. Stanford University, August 18, 2021. https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept.

Creemers, Rogier. “China’s Cyber Governance Institutions,” Leiden Asia Center, January 2021, 1–22.

Creemers, Rogier. China’s Approach to Cyber Sovereignty. Berlin, Germany: Konrad-Adenauer-Stiftung, 2020.

DREZNER, DANIEL W. “The Global Governance of the internet: Bringing the State Back In.” Political Science Quarterly 119, no. 3 (2004): 477–98. https://doi.org/10.2307/20202392.
Drinhausen, Katya, Mikko Huotari, John Lee, and Helena Legarda. “THE CCP'S NEXT CENTURY Expanding Economic Control, Digital Governance and National Security.” Edited by Nis Grunberg and Claudia Wessling. Berlin, 2021.

Dudley, Lauren, Graham Webster, Rogier Creemers, and Elsa Kania, trans. “Translation: Cybersecurity Review Measures.” DigiChina. Stanford University, July 2, 2021. https://digichina.stanford.edu/news/translation-cybersecurity-review-measures.

Dudley, Lauren, Graham Webster, Rogier Creemers, and Elsa Kania. “China's Cybersecurity REVIEWS EYE 'Supply Chain Security' in 'Critical' Industries [Translation].” Cybersecurity Initiative. New America, April 27, 2020. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-eye-supply-chain-security-critical-industries-translation/.

Eisentraut, Sophie. “Talking Democracy at the United Nations.” ProQuest EBook Central, 2020, 61–73. https://doi.org/10.5771/9783748909347.

Epstein, Dmitry. “The Making of Institutions of Information Governance: The Case of the Internet Governance Forum.” Journal of Information Technology 28, no. 2 (2013): 137–49. https://doi.org/10.1057/jit.2013.8.

Fidler, David P. “Cyberspace and Human Rights.” Research Handbook on International Law and Cyberspace, n.d., 94–117. https://doi.org/10.4337/9781782547396.00014.

Finnemore, Martha, and Duncan B. Hollis. “Constructing Norms for Global Cybersecurity.” American Journal of International Law 110, no. 3 (2016): 425–79. https://doi.org/10.1017/s0002930000016894.

Finnemore, Martha, and Kathryn Sikkink. “International Norm Dynamics and Political Change.” International Organization 52, no. 4 (1998): 887–917. https://doi.org/10.1162/002081898550789.

Finnemore, Martha. “International Organizations as Teachers of Norms: The United Nations Educational, Scientific, and Cutural Organization and Science Policy.” International Organization 47, no. 4 (1993): 565–97. https://doi.org/10.1017/s0020818300028101.

Fliegauf, Mark T. “In Cyber (Governance) We Trust.” Global Policy 7, no. 1 (2016): 79–82. https://doi.org/10.1111/1758-5899.12310.

FLONK, DANIËLLE, MARKUS JACHTENFUCHS, and ANKE S. OBENDIEK. “Authority Conflicts in internet Governance: Liberals vs. Sovereigntists?” Global Constitutionalism 9, no. 2 (2020): 364–86. https://doi.org/10.1017/s2045381720000167.

Foot, Rosemary. "'Doing Some Things' in the Xi Jinping Era: The United Nations as China's Venue of Choice." International Affairs (London) 90, no. 5 (2014): 1085-100.

Gavrilovic , Andrijana, and Ilona Stadnik. “3Rd Meeting of the First SUBSTANTIVE Session of the Open-Ended Working Group (Oewg).” 3rd Meeting of the first substantive session of the Open-Ended Working Group (OEWG) | Digital Watch. Digital Watch, 2019. Accessed August 29, 2021. https://dig.watch/resources/3rd-meeting-first-substantive-session-open-ended-working-group-oewg.

Gavrilovic, Andrijana, and Ilona Stadnik. “6Th Meeting of the First SUBSTANTIVE Session of the Open-Ended Working Group (Oewg).” 6th Meeting of the first substantive session of the Open-Ended Working Group (OEWG) | Digital Watch. Digital Watch, 2019. https://dig.watch/resources/6th-meeting-first-substantive-session-open-ended-working-group-oewg.

Gavrilović, Andrijana. “4Th Meeting of the First SUBSTANTIVE Session of the Open-Ended Working Group (Oewg).” 4th Meeting of the first substantive session of the Open-Ended

Working Group (OEWG) | Digital Watch. Digital Watch, 2019. https://dig.watch/resources/4th-meeting-first-substantive-session-open-ended-working-group-oewg.

Gavrilovic, Andrijana. "A New Landmark in Global Cybersecurity Negotiations: UN Cyber OEWG in Numbers." www.diplomacy.edu. DiploFoundation, March 18, 2021. https://www.diplomacy.edu/blogs/new-landmark-global-cybersecurity-negotiations-un-cyber-oewg-numbers/.

Gavrilović, Andrijana. "Confidence-Building Measures." Confidence-building measures | Digital Watch. Digital Watch, 2020. https://dig.watch/sessions/confidence-building-measures.

Gellman, Barton, and Laura Poitras. "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program." The Washington Post. WP Company, June 7, 2013. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

Gierow, Hauke Johannes Gierow. "Cyber Security in China: New Political Leadership Focuses on Boosting National Security." China Monitor- Merics 20 (December 2014): 1–9.

Gierow, Hauke. "China's March towards CYBER Hegemony." China's march toward cyber hegemony. Merics, October 8, 2018. https://merics.org/en/analysis/chinas-march-towards-cyber-hegemony.

Gill, Amandeep S. "The Changing Role of Multilateral Forums in Regulating Armed Conflict in the Digital Age." International Review of the Red Cross 102, no. 913 (2020): 261–85. https://doi.org/10.1017/s1816383121000059.

Glen, Carol M. "internet Governance: Territorializing Cyberspace?" Politics & Policy 42, no. 5 (2014): 635–57. https://doi.org/10.1111/polp.12093.

Goel, Sanjay. "National Cyber Security Strategy and the Emergence of Strong Digital Borders." Connections: The Quarterly Journal 19, no. 1 (2020): 73–86. https://doi.org/10.11610/connections.19.1.07.

Greenwald, Glenn, and Ewan MacAskill. "NSA PRISM PROGRAM TAPS in to User Data of Apple, Google and Others." The Guardian. Guardian News and Media, June 7, 2013. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Gu Zuxue. "SPECIAL ISSUE： RULE OF LAW--CHINA AND THE WORLD International Law as the Law of Domestic Governance： China＇s Propositions and Institutional Practice." Social Sciences in China 38, no. 3 (2017): 157-74.

Han, Tongyun, and Yuhang Zhang. "Comment and Analysis on the Major National Strategies of Cyberspace." World Scientific Research Journal 6, no. 5 (2020): 275–81. https://doi.org/10.6911/WSRJ.202005_6(5).0029.

Haugen, Hans Morten. “The Crucial and Contested Global Public Good: Principles and Goals in Global internet Governance.” internet Policy Review 9, no. 1 (2020): 1–22. https://doi.org/10.14763/2020.1.1447.

Henderson, Christian. “THE UNITED NATIONS AND THE REGULATION OF CYBERSECURITY.” Essay. In RESEARCH Handbook on International Law and Cyberspace, 1–25. Cheltenham, UK: EDWARD ELgeneral assemblyR PUBLISHING, 2021.

Henderson, Christian. “The United Nations and the Regulation of Cyber-Security.” Research Handbook on International Law and Cyberspace, 2015, 465–90. https://doi.org/10.4337/9781782547396.00035.

Hoffman, Paul. “The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force.” Internet Engineering Task Force Trust. IETF, November 2012. http://www2.cs.uh.edu/~gnawali/courses/cosc6377-f12/ietf-tao.pdf.

Hofmann, Jeanette, Christian Katzenbach, and Kirsten Gollatz. “Between Coordination and Regulation: Finding the Governance in internet Governance.” New Media & Society 19, no. 9 (2016): 1406–23. https://doi.org/10.1177/1461444816639975.

Huang, Zhixiong, and Yaohui Ying. “The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective.” International Review of the Red Cross 102, no. 913 (2020): 335–65. https://doi.org/10.1017/s1816383121000023.

Ittelson, Pavlina. “3Rd Meeting of the THIRD SUBSTANTIVE Session of the Open-Ended Working Group (Oewg).” 3rd Meeting of the third substantive session of the Open-Ended Working Group (OEWG) | Digital Watch. Digital Watch, 2021. Accessed August 29, 2021. https://dig.watch/resources/3rd-meeting-third-substantive-session-open-ended-working-group-oewg.

Ittelson, Pavlina. “9Th Meeting of the Third Session of the Open-Ended Working Group (Oewg).” 9th Meeting of the third session of the Open-Ended Working Group (OEWG) | Digital Watch. Digital Watch, 2021. https://dig.watch/resources/9th-meeting-third-session-open-ended-working-group-oewg.

Ittelson, Pavlina. “International Law.” International law . Digital Watch, 2020. https://dig.watch/sessions/international-law.

Ittelson, Pavlina. “What's New with Cybersecurity Negotiations? Un Cyber Oewg Final Report Analysis.” Diplo. Diplo Foundation, August 10, 2021. https://www.diplomacy.edu/blog/whats-new-cybersecurity-negotiations-un-cyber-oewg-final-report-analysis#discussion.

Ittelson, Pavlina. Capacity building. Digital Watch, 2020. https://dig.watch/sessions/capacity-building.

Kaska, Kadri, and Maria Tolppa. “Brief; China's Sovereignty and internet Governance.” Tallinn: Estonia Foreign Policy Institute, 2020.

Kastner, Philipp, and Frédéric Mégret. “International Legal Dimensions of Cybercrime.” Research Handbook on International Law and Cyberspace, 2015, 190–208. https://doi.org/10.4337/9781782547396.00019.

Katz, Heather L. “internet Access and Freedom: Constructing and Reacting to Transnational Norms about internet Diffusion and Use.” Dissertation, ProQuest, 2016.

Katzenstein, Peter J. , editor, 1967, "The Culture Of National Security: Norms And Identity In World Politics" (1996). *Books by Alumni*. 4080. https://works.swarthmore.edu/alum-books/4080

Klein, Hans. “ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy.” The Information Society 18, no. 3 (2002): 193–207. https://doi.org/10.1080/01972240290074959.

Kohl, Uta. “Jurisdiction in Cyberspace.” Research Handbook on International Law and Cyberspace, 2015, 30–54. https://doi.org/10.4337/9781782547396.00011.

Kong, Qingjiang. "Beyond the Love–Hate Approach?: International Law and International Institutions and the Rising China." China (National University of Singapore. East Asian Institute) 15, no. 1 (2017): 41-62.

Lantis, Jeffrey S, and Daniel J Bloomberg. “Changing the Code? NORM Contestation and US Antipreneurism in Cyberspace.” International Relations 32, no. 2 (2018): 149–72. https://doi.org/10.1177/0047117818763006.

Laskai, Lorand, and Graham Webster. “Translation: Chinese Expert Group OFFERS 'GOVERNANCE Principles' for 'RESPONSIBLE AI'.” Cybersecurity Initiative. New America, June 17, 2019. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-expert-group-offers-governance-principles-responsible-ai/.

Lin, Ying Yu. “China Cyber Warfare and Cyber Force.” Tamkang Journal of International Affairs, China Cyber Warfare and Cyber Force, 22, no. 3 (2018): 119–61.

Lu, Hong, Bin Liang, and Melanie Taylor. “A Comparative Analysis of Cybercrimes and Governmental Law Enforcement in China and the United states.” Asian Journal of Criminology 5, no. 2 (2010): 123–35. https://doi.org/10.1007/s11417-010-9092-5.

MARCH, JAMES G., and JOHAN P. OLSEN. “Institutional Perspectives on Political Institutions.” Governance 9, no. 3 (1996): 247–64. https://doi.org/10.1111/j.1468-0491.1996.tb00242.x.

Maurer, Tim. “A Dose of Realism: The Contestation and Politics of Cyber Norms.” Hague Journal on the Rule of Law 12, no. 2 (2019): 283–305. https://doi.org/10.1007/s40803-019-00129-8.

Meyer, Paul, and Daniel Stauffacher. “ICT4PEACE AND THE UNITED NATIONS OPEN-ENDED WORKING GROUP ON INTERNATIONAL CYBERSECURITY (UN OEWG) 2019-2021.” Geneva: ICT4Peace Foundation, 2021.

Miao, Weishan, and Peng Hwa Ang. “internet Governance: From the Global to the Local.” Communication and the Public 1, no. 3 (2016): 377–84.

Miao, Weishan, Min Jiang, and Yunxia Pang. “Historicizing internet Regulation in China: A Meta-Analysis of Chinese internet Policies (1994-2017).” International Journal of Communication 15 (2021): 2003–26.

Nasu, Hitoshi, and Helen Trezise. “Cyber Security in the Asia-Pacific.” Research Handbook on International Law and Cyberspace, n.d., 446–64. https://doi.org/10.4337/9781782547396.00034.

Noesselt, Nele. “Microblogs and the Adaptation of the Chinese PARTY-STATE'S Governance Strategy.” Governance 27, no. 3 (2013): 449–68. https://doi.org/10.1111/gove.12045.

Pawlak, Patryk. “Capacity Building in Cyberspace as an Instrument of Foreign Policy.” Global Policy 7, no. 1 (2016): 83–92. https://doi.org/10.1111/1758-5899.12298.

Rafaelof, Emma, Rogier Creemers, Samm Sacks, Katharin Tai, Graham Webster, and Kevin Neville. “Translation: China's 'Data Security Law (Draft)'.” Cyberecurity Initiative. New America, July 2, 2020. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/.

Rahmatian, Andreas. “Cyberspace and Intellectual Property Rights.” Research Handbook on International Law and Cyberspace, n.d., 72–93. https://doi.org/10.4337/9781782547396.00013.

Ronaghan, Stephen A. “Benchmarking E-government: A Global Perspective.” New York, New York: United Nations, 2002

Ruhl, Christian, Duncan Hollis, Wyatt Hoffman, and Tim Maurer. “Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads.” Carnegie Endowment for International Peace , February 2020, 1–32.

Sacks, Samm. “China's Emerging Cyber Governance System.” China's Emerging Cyber Governance System | Center for Strategic and International Studies. Center for Strategic and International Studies, 2021. https://www.csis.org/chinas-emerging-cyber-governance-system.

Saul, Ben, and Kathleen Heath. “Cyber Terrorism.” Research Handbook on International Law and Cyberspace, n.d., 147–67. https://doi.org/10.4337/9781782547396.00017.

Schmitt, Michael. “The Sixth GGE and International Law in Cyberspace.” Just Security. New York University School of Law, June 11, 2021. https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.

Segal, Adam. “China’s Alternative Cyber Governance Regime.” Washington DC: Council for Foreign Relations, March 13, 2020.

Shackelford, Scott J., Enrique Oti, Jaclyn A. Kerr, Elaine Korzak, and Andreas Kuehn. "Back to the Future of Internet Governance," Georgetown Journal of International Affairs 16, no. Special Issue (2015): 83-97

Shi, Mingli. “What China's 2018 internet Governance Tells Us about What's Next.” Cybersecurity Initiative. New America, January 28, 2019. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/what-chinas-2018-internet-governance-tells-us-about-whats-next/.

Soesanto, Stefan, and Fosca D’Incau. “The UN GGE Is Dead: Time to Fall Forward.” European Power. European Council on Foreign Relations, August 15, 2017. https://ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance/.

Stadnik, Ilona. “10Th Meeting of the Third Session of the OEWG.” 10th Meeting of the third session of the OEWG | Digital Watch. Digital Watch, 2021. https://dig.watch/resources/10th-meeting-third-session-oewg.

Stadnik, Ilona. “2Nd Meeting of the THIRD SUBSTANTIVE Session of the Open-Ended Working Group (Oewg).” 2nd Meeting of the third substantive session of the Open-Ended Working Group (OEWG) | Digital Watch. Digital Watch, 2021. Accessed August 29, 2021. https://dig.watch/resources/2nd-meeting-third-substantive-session-open-ended-working-group-oewg-0.

Stadnik, Ilona. “4Th Meeting of the THIRD SUBSTANTIVE Session of the Open-Ended Working Group (Oewg).” 4th Meeting of the third substantive session of the Open-Ended Working Group (OEWG) | Digital Watch. Digital Watch, 2021. https://dig.watch/resources/4th-meeting-third-substantive-session-open-ended-working-group-oewg.

Stadnik, Ilona. “5Th Meeting of the First SUBSTANTIVE Session of the Open-Ended Working Group (Oewg).” 5th Meeting of the first substantive session of the Open-Ended Working Group (OEWG) | Digital Watch. Digital Watch, 2019. https://dig.watch/resources/5th-meeting-first-substantive-session-open-ended-working-group-oewg.

Stadnik, Ilona. “Norms, Rules and Principles.” Norms, rules and principles . Digital Watch, 2020. https://dig.watch/sessions/norms-rules-and-principles.

Stadnik, Ilona. Regular institutional dialogue. Digital Watch, 2020. https://dig.watch/sessions/regular-institutional-dialogue.

Sunstein, Cass R. "Social Norms and Social Roles," 96 Columbia Law Review 903 (1996)

Tanczer, Leonie Maria, Irina Brass, and Madeline Carr. “CSIRTs and GLOBAL Cybersecurity: How Technical EXPERTS Support Science Diplomacy.” Global Policy 9 (2018): 60–66. https://doi.org/10.1111/1758-5899.12625.

Tikk, Eneken, and Mika Kerttunen. “Parabasis; Cyber Diplomacy in Stalemate.” Oslo: Norwegian Insitute of International Affairs, May 2018.

Tikk-Ringas, Eneken. “International Cyber Norms Dialogue as an Exercise of Normative Power.” Georgetown Journal of International Affairs 17, no. 3 (2016): 47–59. https://doi.org/10.1353/gia.2016.0036.

Tsagourias, Nicholas. “The Legal Status of Cyberspace.” Research Handbook on International Law and Cyberspace, 2015, 13–29. https://doi.org/10.4337/9781782547396.00010.

United Nations General Assembly. *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 (A/66/359). New York, NY; United Nations, 2011.*

United Nations General Assembly. *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/69/723). New York, NY; United Nations, 2015.*

United Nations General Assembly. *Resolution adopted by the General Assembly on 5 December 2018 (A/RES/73/27).* New York, NY; United Nations, 2018.

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/76/135)*. New York, NY; United Nations, 2021.

The Standing Committee of the People’s Congress. “Cybersecurity Law of the People's Republic of China.” Translated by THE CHINA NGO PROJECT. ChinaFile. THE CHINA NGO PROJECT, October 16, 2019. Originally published 2016. https://www.chinafile.com/ngo/laws-regulations/cybersecurity-law-of-peoples-republic-of-china.

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)*. New York, NY; United Nations, 2015.

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *Report of the Group of*

Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201). New York, NY; United Nations, 2010.

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98)*. New York, NY; United Nations, 2013.

United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security. *Final Report (A/AC.290/2021/CRP.2)*. New York, NY; United Nations, 2021.

United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security. *Compendium of statements in explanation of position on the final report (A/AC.290/2021/INF/2)*. New York, NY; United Nations, 2021.

United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security. *Draft Substantive Report (Zero Draft) [A/AC.290/2021/L.2]*. New York, NY; United Nations, 2021.

United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security. *Joint proposal by a group of states to the Chair of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York, NY; United Nations, 2021.

United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security. *China's Contribution on the Zero Draft of the OEWG Substantive Report*. New York, NY; United Nations, 2021.

van Eeten, Michel JG, and Milton Mueller. "Where Is the Governance in internet Governance?" New Media & Society 15, no. 5 (2012): 720–36. https://doi.org/10.1177/1461444812462850.

Webster, Graham, ed. "Translation: Cybersecurity Review Measures (Revised, Draft for Comment) - July 2021." Translated by Rogier Creemers. DigiChina. Stanford University, July 12, 2021. https://digichina.stanford.edu/news/translation-cybersecurity-review-measures-revised-draft-comment-july-2021.

Wei Liu. 2014. China In The United Nations. Hackensack, NJ: World Century Publishing Corporation. http://search.ebscohost.com.ezproxy.leidenuniv.nl:2048/login.aspx?direct=true&db=e000xww&AN=779668&site=ehost-live.

Weiss, Jessica Chen, and Jeremy Wallace. “Domestic Politics, China’s Rise, and the Future of the Liberal International Order.” International Organization 75 (2021): 635–64. https://doi.org/10.2139/ssrn.3671848.

White, Paul Antony. “Cyberpeace: Why internet Governance Matters for Global Peace and Stability.” Peace & Change 44, no. 4 (2019): 441–67. https://doi.org/10.1111/pech.12373.

Whitmore, Andrew, Namjoo Choi, and Anna Arzrumtsyan. “One Size Fits All? On the Feasibility of International internet Governance.” Journal of Information Technology & Politics 6, no. 1 (2009): 4–11. https://doi.org/10.1080/19331680802664127.

WILSON, ERNEST J. “What Is internet Governance and Where Does It Come from?” Journal of Public Policy 25, no. 1 (2005): 29–50. https://doi.org/10.1017/s0143814x0500019x.

Yang, Yi Edward. “China’s Strategic Narratives in Global Governance Reform under Xi Jinping.” Journal of Contemporary China 30, no. 128 (2020): 299–313. https://doi.org/10.1080/10670564.2020.1790904.

Yang, Yifan. “The internet AND China’s Foreign Policy Decision-Making.” Chinese Political Science Review 1, no. 2 (2016): 353–72. https://doi.org/10.1007/s41111-016-0021-3.

Yoo, Joonkoo. “UN Open-Ended Working Group Final Report: Issues and Implications .” Translated by Kyungmin An. IFANS Focus, 2021, 1–3.

Zeng, Jinghan, Tim Stevens, and Yaru Chen. “China's Solution to Global CYBER Governance: Unpacking the Domestic Discourse OF ‘INTERNET SOVEREIGNTY.’” Politics & Policy 45, no. 3 (2017): 432–64. https://doi.org/10.1111/polp.12202.

Zheng, Junsong, and Siyu Hou. “Promoting the Construction of Party Style and Clean Government in Colleges and Universities with Chinese Traditional Family Style under the Era of ‘internet plus.’” International Journal of Social Science and Education Research 3, no. 11 (2020): 106–11. https://doi.org/DOI: 10.6918/IJOSSER.202011_3(11).0019.

Appendices

Appendix A; Checklist for Analyses

	checklist citations		gge 2010		gge 2013		gge 2015		oewg 2021		gge 2021	
	*explicitly stated	THREATS										
1	China's Working Paper (I.1)	cyber attack, crime, terrorism		6*	x	6*, 7*	x	6*, 7*	x	15, 16*	x	13*, 14*
2	China's Working Paper (I.2)	weaponizing cyberspace/ increased mil applications of tech	x	7*			x	4*	x	16*	x	7*
3	China's Working Paper (I.3)	cyber attack on CI/CII	x	9	x	9	x	5*	x	18*	x	10*
4	China's Working Paper (I.4)	Fake News (applicable 2019 forward)									x	9*
5	China's Working Paper (I.4)	personal data abuse										
6	China's Working Paper (I.5)	politicization of tech and cybersecurity										
7	China's Working Paper (I.6)	tech developments = new risks	x	9*	x	5	x	3	x	15*	x	11*
8	China's Working Paper (I.7)	imbalanced management of critical internet										

	checklist citations		gge 2010		gge 2013		gge 2015		oewg 2021		gge 2021	
		infrastructure										
9	China's Working Paper (1.7)	increasing digital divide	x	11*	x	10*	x	8*	x	11, 20*, 21*	x	12*
		NORMS										
10	initial non paper// China's Working Paper (II.ii)// Code of conduct 2011 (b)// Code of conduct 2015 (2.2)// Internet White paper 2010 (V para 2)	no use of ICT by any state that would undermine int'l peace/security	-	-	x	19, 23	x	13*a, c, f	x	24*	x	(13a, c, f), 20*
11	initial non paper// China's Working Paper (II.ii.1)// Code of conduct 2011 (e)// Code of conduct 2015 (2.6)// Internet White paper 2010 (V para 1)*	state jurisdiction/ sovereignty of ICT infrastructure, resources, and activities w/in territory	-	-	x	20*	x	27*, 28*a			x	71b*
12	initial non paper// China's Working Paper (II.ii.2)// Code of conduct 2015 (2.7.a,b)// Internet White paper 2010 (V para 3)	state's right to make ICT policy consistent with national circumstances	-	-								
13	// Code of conduct 2011 (f)//// Code of conduct 2011 (e)// Code of conduct 2015 (2.7.a,b)// Internet White paper 2010 (V para 3)	information available on the internet based on the relevant national laws and regulations including nat'l sec and public order	-	-								
14	initial non paper// China's Working Paper (II.ii.3)//	no state interference using ICT technology	-	-	x	19, 20, 23	x	13* f	x	31	x	(13c, f), 20*,71*c

	checklist citations		gge 2010		gge 2013		gge 2015		oewg 2021		gge 2021	
	Code of conduct 2011 (b)// Code of conduct 2015 (2.3)// Internet White paper 2010 (V para 2)											
15	initial non paper// China's Working Paper (II.ii.4)// Internet White paper 2010 (VI para 3)*	equal management of internet infra/resources	-	-								
16	initial non paper// China's Working Paper (II.iii.1)// Code of conduct 2011 (e)// Code of conduct 2015 (2.6)// Internet White paper 2010 (IV para 4)*	state has the right/responsibility of legal protection of ICT	-	-			x	13g			x	(13g),44*, 47
17	initial non paper// China's Working Paper (II.iii.2)// Code of conduct 2011 (b)// Code of conduct 2015 (2.2)// Internet White paper 2010 (V para 2)	no cyberattacks on CI/CII	-	-			x	13*f	x	31*	x	(13 f*),20
18	initial non paper// China's Working Paper (II.iii.3)// Code of conduct 2011 (d)// Code of conduct 2015 (2.3)// Internet White paper 2010 (V para 2)	do not use policy/technological advantage to undermine other states' CI	-	-			x	13f	x	31	x	(13f)
19	initial non paper// China's Working Paper (II.iii.4)// Internet White paper 2010 (VI para 4)	increase exchanges on standards/best practices related to protecting CI	-	-			x	13d	x	31*	x	(13d)
20	initial non paper// China's Working Paper (II.iv.1)//	Balanced approach to technical advancement,	-	-								

	checklist citations		gge 2010		gge 2013		gge 2015		oewg 2021		gge 2021	
	Internet White paper 2010 (IV para 3)	business development, public interests, and national security										
21	// Code of conduct 2011 (h)//// Code of conduct 2011 (e)// Code of conduct 2015 (2.9)// Internet White paper 2010 (IV para 5)	states should be the leaders of infosec and educate other relevant sectors	-	-								
22	initial non paper // China's Working Paper (II.iv.2)// Code of conduct 2011 (e)// Code of conduct 2015 (2.6)// Internet White paper 2010 (IV para 4)	states have the right/responsibility to ensure security of critical data	-	-			x	13g			x	(13g), 44*, 47
23	initial non paper// China's Working Paper (II.iv.3)// Code of conduct 2011 (b)// Code of conduct 2015 (2.2,3)	No ICT enabled espionage that results in important data theft/ mass surveillance	-	-			x	13c, f	x	31	x	(13c, f), 20, 37*
24	initial non paper// China's Working Paper (II.iv.4)// Internet White paper 2010 (IV para 1)	equal attention to development/security as well as lawful, orderly, free flow of data	-	-								
25	initial non paper// China's Working Paper (II.iv.4)// Internet White paper 2010 (VI para 4)	exchange of best practices/cooperation for ^	-	-			x	13d			x	(13d)
26	initial non paper// China's Working Paper (II.v.1)// Code of conduct 2011 (d)// Code of conduct 2015 (2.5)	no blocking independent state control of ICT goods, services, and security	-	-			x	13f	x	31	x	(13f)

	checklist citations		gge 2010		gge 2013		gge 2015		oewg 2021		gge 2021	
27	initial non paper// China's Working Paper (II.v.2) Code of conduct 2011 (d)// Code of conduct 2015 (2.5)// Internet White paper 2010 (V para 4/5)	no illegal attainment of data	-	-			x	13i	x	28	x	(13i), 58*
28	initial non paper// China's Working Paper (II.v.2) Code of conduct 2011 (d)// Code of conduct 2015 (2.5)// Internet White paper 2010 (V para 4/5)	no backdoors	-	-			x	13i	x	28	x	(13i), 58*
29	initial non paper// China's Working Paper (II.v.2) Code of conduct 2011 (d)// Code of conduct 2015 (2.5)	no forced upgrades	-	-								
30	initial non paper// China's Working Paper (II.v.2))//	disclose the vulnerabilities if found	-	-			x	13j*	x	28	x	(13j*)
31	initial non paper// China's Working Paper (II.v.3)// Code of conduct 2011 (d)// Code of conduct 2015 (2.5)	no limiting market access of ICT based on nat'l security concerns	-	-			x	13i	x	28	x	(13i)
32	Code of conduct 2011 (d)// Code of conduct 2015 (2.5)	supply chain security to be secured	-	-	x	8	x	13i*	x	28*	x	(13i*), 56*
33	initial non paper// China's Working Paper (II.vi.1)// Code of conduct 2011 (c)// Code of conduct 2015 (2.4)// Internet White paper 2010 (IV para 6)	disallow terrorist recruitment/content on the internet	-	-	x	22*	x	13h			x	(13h)

	checklist citations		gge 2010		gge 2013		gge 2015		oewg 2021		gge 2021	
34	initial non paper// China's Working Paper (II.vi.2)// Code of conduct 2015 (2.4)// Internet White paper 2010 (VI para 4)	intelligence/law enforcement exchanges and cooperation on counter terrorism	-	-	x	22*	x	13d*, h			x	(13d*, h), 31*, 51
35	initial non paper// China's Working Paper (II.vi.3)// Code of conduct 2015 (2.4)// Internet White paper 2010 (VI para 4)	cooperate within international organizations to fight counter terrorism	-	-			x	13d, h			x	(13d*, h), 31*
36	initial non paper// China's Working Paper (II.vi.4)// Code of conduct 2011 (c)// Code of conduct 2015 (2.4)// Internet White paper 2010 (IV para 6)	ISP should close down terrorist websites	-	-								
37	China's Working Paper (II.vii)	further study on the norms/rules/principles of cyberspace	-	-			x	9*, 15*	x	29*		
38	// Code of conduct 2011 (j)// Code of conduct 2015 (2.12)// Internet White paper 2010 (VI para 3)	UN should be promoted for 'prominent role' in creating norms for info sec	-	-	x	13*	x	33*, 34*			x	96*, 97*
		APPLICATION OF INT'L LAW (the following should apply)										
39	China's Working Paper (III.1)// Code of conduct 2011 (a)// Code of conduct 2015 (2.1)// Internet White paper 2010 (V para 1)	sovereign equality/sovereignty	-	-	x	19, 20*	x	24, 25, 26*	x	34	x	69, 70*

	checklist citations		gge 2010		gge 2013		gge 2015		oewg 2021		gge 2021	
40	China's Working Paper (III.1,2)// Code of conduct 2011 (a,k)// Code of conduct 2015 (2.1,13)	no use of force	-	-	x	19	x	24, 25, 26*	x	34	x	69, 70*
41	China's Working Paper (III.1,2)// Code of conduct 2011 (a,k)// Code of conduct 2015 (2.1,13)	peaceful resolution	-	-	x	19	x	24, 25, 26*	x	34, 35*	x	69, 70*, 71a*
42	China's Working Paper (III.1)// Code of conduct 2011 (a)// Code of conduct 2015 (2.1)	non-interference with other states	-	-	x	19	x	24, 25, 26*	x	34	x	69, 70*
43	China's Working Paper (III.3)	do not legalize cyberwarfare by creating guidelines for it	-	-								negated 71f
44	China's Working Paper (III.4)	creation of a separate int'l legal institution for ICT related issues (such as convention for cybercrime/terrorism etc.)	-	-								
		CBM										
45	China's Working Paper (IV)// Code of conduct 2015 (2.10)// Internet White paper 2010 (VI para 4)	policy/tech exchange	-	-	x	26*b, e, f	x	16*b, di, 17*a			x	76?, 82, 83*, 90*
46	China's Working Paper (IV// Code of conduct 2015 (2.10)// Internet White paper 2010 (VI para 4)	Info sharing	x	18iii	x	26*a, c, d, e, f, 27*	x	16*a, b, c, dii, 17*a,	x	48*, 50*, 52*	x	78*, 79*, 81*, 84?

	checklist citations		gge 2010		gge 2013		gge 2015		oewg 2021		gge 2021	
								b, e				
		CAPACITY BUILDING MEASURES										
47	China's Working Paper (V.1)// Code of conduct 2011 (i)// Code of conduct 2015 (2.11)	increase financial and technological assistance to developing countries	-	-	x	31, 32*a, d	x	21c*	x	66*	x	89d*, f*, 90*
48	China's Working Paper (V.2)	publish vulnerabilities or threats asap, as detected	-	-			x	13j*			x	(13j*), 60*
49	China's Working Paper (V.3) // Code of conduct 2011 (g)// Code of conduct 2015 (2.8)// Internet White paper 2010 (VI para 3)	multilateral, democratic, transparent governance system for cyber	-	-								
50	China's Working Paper (V.3)// Code of conduct 2011 (g)// Code of conduct 2015 (2.8)// Internet White paper 2010 (VI para 3)	critical internet resources should be separate from the influence of any state	-	-								
		INSTITUTIONAL DIALOGUE										
51	China's Working Paper (VII)	welcomes permanent process within UN framework to deal with cyber issues	-	-								
			-	-								
		total of checklist included out of 51	6	11%	18	35%	34	66%	24	47%	34	66%

	checklist citations		gge 2010		gge 2013		gge 2015		oewg 2021		gge 2021	
		total of checklist that is explicit	4	8%	10	20%	22	43%	13	25%	28	55%
		percent of JUST norms included	-	-	7/28	33%	21/28	75%	13/28	46%	20/28	71%
		percent of JUST EXPLICIT norms included	-	-	4/28	14%	10/28	36%	5/28	18%	14/28	50%

Appendix B; Figure 7, 2021 GGE highlighted summary

Figure 7; 2021 highlighted summary of 2015 est. Cyber Norms (A/76/135, clauses 19-73)

- States should cooperate to stabilize and secure ICT
  - Previous measures of the GGE and OEWG are the base for responsible state behavior in cyberspace
- States should consider relevant information regarding ICT incident attribution
  - Use all information available to avert misunderstandings and escalating tensions
  - States are encouraged to consult with competent authorities within ICT incidents
  - States that fall victim to ICT incidents should consult all possible information
  - States response to ICT incidents should fall within international obligations to the UN
  - Regional and international cooperation is encouraged before reaching a conclusion on an ICT incident
- States should not knowingly use territory for malicious ICT acts
  - States should take all available measures to stop malicious ICT acts once aware or notified
  - States should take reasonable steps to monitor and end these activities
  - States should seek assistance if unable to combat the threat themselves
  - Affected states should notify the origin state of the ICT threat and it should be acknowledged as well as combated
  - Origin of an ICT incident does not indicate responsibility
- States should consider widespread cooperation to address ICT threats
  - Observance of this norm includes the institutionalization of this cooperation

    - States should strengthen and develop methods of information exchange
- States should recognize human rights specific to the internet
    - States should protect and recognize human rights and fundamental freedoms both offline and online
    - Arbitrary or unlawful mass surveillance harms human rights
    - States should consider guidance from previous resolutions on cyber norms and human rights
    - Respect for human rights should be built in to responsible and secure use of ICTs
    - States should invest in measures for a more inclusive and accessible ICT environment
    - States should utilize UN fora and various stakeholders to decrease negative impacts of ICT policy
- States should not support actions that harm CI/CII
    - Actions that harm CI/CII have a cascading effect and could lead to conflict
    - CI/CII are national assets and any damage will have significant impact on all aspects of the state and society
    - Each state determines what is CI/CII within their own state
    - Covid-19 has highlighted the importance of protecting healthcare within this category of CI/CII
    - States are encouraged to make and implement national policy in line with this norm
- States should take measures to protect their CI/CII
    - States should designate their CI/CII and implement national legislation to protect it
    - States should cooperate with cross border ICT hosts to enhance ICT security
- States should respond to requests from states whose CI/CII has been damaged
    - Cooperation, dialogue, and respect for sovereignty should be central
    - States should offer all possible and reasonable assistance to any request
    - Establishing structures and mechanisms to this end is encouraged
    - Common templates and processes are encouraged to facilitate cooperation
    - Assistance with these requests can repair trust where applicable
- States should take measures to secure the supply chain of ICT products
    - End user confidence should be ensured to protect international security and broader economic development
    - Reasonable steps to secure the supply chain include the establishment of frameworks, mechanisms, policies, programs, dialogues, and exchange of good practice.
    - States should consider national measures to prevent the spread of malicious ICT practices
- States should prevent use of malicious ICT tools and hidden functions
    - States should consider national measures to prevent the spread of malicious ICT practices
- States should encourage responsible reporting of ICT vulnerabilities
    - Quick response means less time for others to exploit discovered vulnerabilities
    - Specific programs and policy for vulnerability disclosure encourage routine reporting

    - Decision making guidelines for handling these vulnerabilities can protect against misuse
    - States should develop incentives and guidance for reporting in conjunction with industry professionals
    - Confidence and capacity building recommendations from previous GGEs should be consulted
- States should not take actions that will harm cyber emergency response teams
    - CERTs are unique and play an important role, and should remain independent and free from politicization
    - CERTs often are considered part of a state's CI
    - States should not use CERTs for malicious reasons and are encouraged to issue a statement regarding this
    - States should consider implementing frameworks to assist CERTs from different nations in cooperation
- States should cooperate with civil society and the private sector to improve ICT security