

# Explaining the U.S. Strategic Narrative Regarding 5G, China and Huawei

Keywords: United States, Huawei, 5G, Strategic Narrative, China

Andréas Almroth Självständigt arbete, 15 hp Statsvetenskap med inriktning krishantering och säkerhet

Handledare: Lindy Newlove Eriksson

Antal ord: 13926

## Index

Index	2
1. Introduction	3
1.1 Research Problem	4
1.2 Aim	6
1.3 Research question	6
1.4 Delimitations	7
2. Theoretical Framework	8
2.1 Previous Research	8
2.2 Strategic Narrative Theory	9
2.3 Criticism of Strategic Narrative Theory	12
2.4 Operationalization	13
2.4.1 Component one: Actors	13
2.4.2 Component two: setting	13
2.4.3 Component three: conflict	14
2.4.4 Component four: suggested resolution	14
3. Method	15
3.1 Research Design	15
3.2 Material	16
4. Analysis	18
4.1 Actors: How does the U.S. portray China and Huawei?	18
4.1.1 The Portrayal of China	18
4.1.2 The Portrayal of Huawei	22
4.2 Setting: How does the U.S. portray the international system?	26
4.3 Suggested Resolution: How does the U.S. portray suggested resolutions?	29
5. Conclusion	32
5.1 Answer to Research Question	32
5.2 Future Research	35
Reference list	36
Books	36
Digital Articles	36

#### 1. Introduction

The term "5G" refers to the fifth generation of wireless communication technology, allowing for wireless internet access at greatly increased transmission speed and decreasing delays in communication networks compared to the previous generation "4G". With the exponential growth in popularity for wireless internet and the connectivity that society depends on, 5G-technology has been in development by communication technology companies and has been deployed on a larger scale since 2019-2020, claiming to be revolutionizing the accessibility and connectivity of our society as a whole (Salih et al, 2020: 2141-2142, 2145). While the specific technological differences between 4G and 5G are rather intricate, the technology essentially allows for the wireless internet access we enjoy today from 4G, to be even more efficiently distributed and allows for massive amounts of data to be shared between communication devices in a matter of seconds (Harrell, 2019: 2-3).

The reason why we might come to rely so much on the development and establishment of 5G-technology in our society is primarily due to the dependency on communication technology that modern societies have developed. Computers and phones connected to the internet are staples in our modern way of living and communicating with others. With the exponential growth in popularity for communication devices and networks, a corresponding demand has emerged for technology that would even further smoothen the communication and interconnectedness of individuals and groups (Salih et al, 2020: 2139-2140).

Huawei is a Chinese communication technology company and currently the biggest smartphone manufacturer in the world. Since 2016, Huawei has been developing 5G-technology, joining the myriad of tech companies that have been competing to develop and establish their technology around the world. Huawei has been enjoying Chinese state backing for some time, which could explain why they've come to be such a big player among the companies that are currently rolling out 5G-technology (Maizland & Chatzky, 2020). For example, Huawei has built roughly 70 percent of the 4G-infrastructure in Africa and likely thanks to China's inclusion of 5G-technology development as part of China's massive "Belt and Road initiative" which has further catapulted Huawei into relevancy (Mackinnon, 2019; Sacks, 2021). By acting as the flag bearer for the Chinese technological advance, diplomacy has played a part in helping Huawei land the contracts that it has, helping to develop communication technology all around the world.

However, concern has primarily been raised in Western states by NATO for example regarding the security risks associated with 5G-technology, particularly when Chinese companies such as Huawei are involved in the installation (Kaska et al, 2019). This fear has risen from the long-standing fact that Chinese companies have had a relation to the Chinese state that is very unlike most other relations between states and companies. Chinese companies are by law required to grant the Chinese government any information it desires from the company, according to article 7 of the National Intelligence Law of the People's Republic of China (2019: 2). This has opened the doors to speculation whether investing and using Chinese technology could mean that customers also open the door to having their information shared with the Chinese state (Federal Communications Commission, 2020).

The ways in which 5G could pose a threat are tied to the increase of digital devices fitted with sensors and means of interconnectedness between devices. This interconnectedness is referred to as the Internet of Things (IoT), where all digital devices are being linked into common networks where information can be gathered and shared between devices. By removing barriers between otherwise separate networks, like radio communication and TV-networks, it could open up innumerable ways in which devices may be accessed through any other device by sharing the same network. If Huawei was to install sensors into their 5G systems, it is feared that this could be exploited in order to extract information or sabotage IT-systems (Friis & Lysne, 2021: 1180-1181, 1190).

#### 1.1 Research Problem

The perceived Chinese telecommunications threat to the United States has increased in the past years, especially in regards to Huawei. In the light of related discussions like possible security threats linked to the popular social media program TikTok, owned by the Chinese company ByteDance, the technology aspect has become an important subject within U.S. security discourse (Figliola, 2020). The Chinese state and China-based companies have come to be portrayed as a monolithic actor which can help in explaining why the discussion about security risks relating to Chinese tech companies is a projection of a larger discussion about Chinese state intentions in the international sphere in general (Maizland & Chatzky, 2020).

Amidst concerns about the possible expansion of Huawei-operated 5G-technology in the United States, then-President Donald Trump issued an executive order in May of 2019 that forbade U.S. companies from using communication and information technology from companies that are labeled as national security threats, an act that has been considered to specifically address the Huawei and 5G-issue (Executive Order - 13873: 2019). In addition, the U.S. Commerce Department had Huawei placed on the "Entity List", joining a list of companies who were thereby essentially banned from acquiring U.S. product components, a deliberate message to Huawei that their presence was unwelcome in U.S. markets (Bureau of Industry and Security, 2020).

This study aims to analyze U.S. perceptions of the Chinese threat in the realm of 5G through using the theory of strategic narrative. The reasons why this is an important field of study are because U.S.-China tensions are on the rise and which means an increase in the societal relevance and academic interest of studies which can develop on the perceptions of danger or narratives from either country (Beckley & Brands, 2021). This explains, for instance, the surge of studies discussing the U.S.-China narrative war about COVID-19, and how that has been able to affect other countries, but also studies which seek to deepen the theoretical knowledge of narratives to better apply the theory to U.S.-China relations (Hagström & Gustafsson, 2021; Breuer & Johnston, 2019). Because U.S.-China tensions have consequences for the world, as it has meant the implementation of legislation in order to combat the perceived Chinese telecommunications threat, it is important to analyze the U.S. narrative regarding China to better understand current and future measures taken against China.

Because this study focuses on the analysis of narratives, the relevant theory chosen for this study is strategic narrative theory, which explains how political leaders use narratives to shape perceptions and behavior in order to attain political goals. The goal of political leaders when using strategic narrative is to increase their influence over other actors. A strategic narrative is successful when other actors accept your framing, which can mean that other actors' interests, identities or perceptions of the system of international relations may align with yours (Miskimmon et al, 2013: 1-2). The reason why this theory is relevant is because it explains how strategic narratives are formed and how they can be broken down in analysis to explain the U.S. perceptions of China and Huawei. Due to the passing and enduring of

legislation against Huawei, it can be assumed that if a strategic narrative has been pushed by the U.S. state, then it has been successful.

The most important reason for why this field of study and theory are of importance is because there seems to be a noteworthy gap in academic knowledge regarding papers that discuss U.S. narratives about 5G. Using the search function of the university-supplied database Anna Lindh Library and Google Scholar with the keywords "Strategic narrative" and "5G", no papers focusing on U.S. and China narratives were found. This is the gap in academic knowledge and research that this study aims to fill.

#### 1.2 Aim

This study aims to analyze the four following government-affiliated documents from 2018-2021: the U.S. National Cyber Strategy (NCS), the Congressional Research Service report titled "Fifth-Generation (5G) Telecommunications Technologies, Issues for Congress", the U.S. Cybersecurity and Infrastructure Security Agency (CISA) document titled "Overview of Risks Introduced by 5G Adoption in the United States", and finally the Interim National Security Strategic Guidance (INSSG). The aim of this study is primarily empirical: to understand the U.S. strategic narrative regarding Chinese-supplied 5G equipment or services to the United States. This study also aims to provide an example of strategic narrative theory being applied to a contemporary empirical case, providing a platform for further in-depth studies regarding the theory and implications of 5G-technology.

#### 1.3 Research question

How can the U.S. perceptions of Huawei and China, in the context of 5G technology, be explained using the theory of strategic narrative?

#### 1.4 Delimitations

The aim of the study is not to detail and analyze the strategic narrative of any other state other than the United States in relation to China. The United States are among the countries that have recognized possible security threats in case 5G-technology was to be implemented in the country by Huawei (Executive Order - 13873: 2019). The aim of the study is not to detail and analyze any other possible actor in this narrative conflict other than China. The relationship between the United States and China also makes it more reasonable to suspect power struggles and narrative conflicts whenever the two countries are involved with one another (Federal Bureau of Investigation, n.d.). This study will mostly focus on the Chinese tech company Huawei. Other Chinese tech companies may be mentioned, like ZTE, however due to the size and success of Huawei, the company has become a standard-bearer for Chinese security scares in Western states, owing to the strong ties between Huawei and the Chinese state (Friis & Lysne, 2021: 1177-1178). It may be more difficult to discern the use of smaller Chinese tech companies for strategic narrative purposes by the United States, companies that might not be as widely recognized.

Sources for the analysis will only consist of government sources. Media sources would be unsuitable as opinions of journalists may not accurately summarize the opinions and conclusions of the U.S towards China. Media sources may also make it difficult to discern broader discourses without having to resort to conducting a quantitative study (Robertson, 2018: 245). The material for the analysis was published in 2018 at its earliest, hence why this study will focus on the time period between 2018 and now (2021), as a more extensive chronological analysis would require more sources from earlier than 2018 and given the relative youth of 5G-technology and the security scare around China and Huawei, the supply is lacking.

#### 2. Theoretical Framework

#### 2.1 Previous Research

Fifth-generation technology is considered to have both immense potential and risk. However, the sheer magnitude of 5G telecommunication systems means a higher security requirement than any previous generations. This explains the immense academic interest in the subject of 5G security which has led to the plethora of research articles that detail security risks with 5G (Ji et al, 2018; Gomez et al, 2012; Shafi et al, 2020; Layton & Witkowski, 2021). For example, a major concern with 5G networks is the increased capability for external actors, such as organized crime groups or state actors, to breach or manipulate data, to carry out denial of service-attacks (DoS) or to hijack identities (Suraci et al: 2021).

There is also a lot of academic interest in China's technological developments and how that may affect other countries' security. China's economy is both large and heavily invested in other countries, which has further sparked academic interest in how China and Chinese companies can influence other states. Since China is also undemocratic, there has often been tensions between some Western states and Chinese companies, such as between the United States and Huawei (Liu, 2020). As a dictatorship that has fewer constraints related to preserving privacy and can use national funds in order to directly fund Huawei's 5G development, China has several advantages in the 5G race. Global dominance of Chinese-supplied 5G can lead to the Chinese government having access to foreign countries' data which can be used for surveillance and would harm U.S. interests (Harold & Kamijima-Tsunoda: 2021).

Furthermore, there has also been research detailing the United States' narrative in different periods of time. One example is a study which examines how the United States' government created a narrative about rogue states being militarily inferior and irrational. The study comes to the conclusion how U.S. defence policymakers framed rogue states as the primary threat to national security, and this narrative subsequently partially led to the justification of the war on terror after 9/11 (Homolar, 2011). Another study regarding the theory of strategic narratives contrasts American and Chinese strategic narratives about the COVID-19 pandemic, but also brings up some criticisms of the theory as the efficacy of strategic narratives remains unclear. Australia, India, South Korea, Turkey and the United Kingdom all

ignored the American and Chinese narratives about the pandemic to instead create their own (Hagström & Gustafsson, 2021).

U.S. concerns about 5G security are very high, especially when the technology is supplied by perceived untrusted Chinese companies such as Huawei. This is also something detailed in previous research. One example is the study by Friis & Lysne (2021) which details how Western actors, such as the EU and the U.S., framed Chinese-supplied 5G as a threat using the theory of securitization. Another example is the article by Radu & Amon (2021) which explains how and why the United States perceives Huawei and other Chinese companies such as ZTE as a threat when it comes to the development and deployment of 5G networks. The article explains that the United States maintains a hard stance against these companies due to path-dependency, meaning the tendency to continue in the direction of past legislation which in the U.S. means legislation that has previously limited security threats posed by Chinese companies, and due to a risk-mitigatory type of governance (Radu & Amon: 2021).

#### 2.2 Strategic Narrative Theory

The theory of strategic narratives was developed as an international relations (IR) theory in the 21st century as a response to the lack of academic attention to how political leaders use narratives to shape perceptions and behavior in order to attain political goals. Strategic narratives are the way in which political leaders can construct a collective meaning of the past, present and future in order to influence internal and external actors (Miskimmon et al, 2013: 1-2).

Platforms through which strategic narratives can be spread include television and social media. States around the world are increasingly financing multilingual transnational television or creating social media accounts, which means political messages spread as part of public diplomacy will reach more people (Miskimmon et al, 2013: 3-4). Strategic narratives are defined by having a clear interest and end goal that are stated by an actor. Strategic narrative theory is inherently constructivist, due to the focus on what is being *portrayed* rather than what *is* (Miskimmon et al, 2013: 5). All strategic narratives use framing, which Robert Entman describes as the "selecting and highlighting some facets of events or issues,

and making connections among them so as to promote a particular interpretation, evaluation, and/or solution" (Entman, 2009: 5).

There are three types of strategic narratives: system narratives (that are about the structure of international relations), identity narratives (that are about the identities of relevant actors according to the actor who portrays a strategic narrative) and issue narratives (the framing of a specific international affair) (Miskimmon et al, 2013: 7). If actor one can, through a strategic narrative, highlight the hypocrisy or unlawfulness of actor two's actions, then the pressure for actor two to change their behavior to be more legitimate may prevail. This is a form of socialization (Miskimmon et al, 2013: 8).

Strategic narrative is in some ways similar to soft power, as soft power similarly emphasizes non-coercive attraction (Miskimmon et al, 2013: 3). Soft power is a term and theory defined by Joseph S. Nye (1990: 167-168), the idea is that states are able to gain influence over other states by aligning their interests with their own. Through cultural, ideological and economical attraction, foreign states become more inclined to approach your interests. All states desire a healthy economy for example, this means that if you cooperate with foreign states through lucrative trade agreements, it is less likely that they will begin to act against your interest because of the benefits that will be lost if they do.

Cultural exportation as a means of exercising soft power can help to portray a country in a positive light for foreign consumers, this could for example be music or a certain idealized lifestyle like the world famous "American Dream". Nye also refers to this as "Co-optive power" and also stresses that more powerful states have greater soft power or co-optive power capabilities, by virtue of their resources and variety of exports (Nye, 1990: 168). This is similar to creating consensus, using strategic narratives, in order to make certain actions more legitimate and others illegitimate. Soft power and strategic narrative are both dissimilar to hard power, which is coercive, and similar because they both focus on spreading norms and values that can influence how others behave (Roselle et al, 2014: 71-72).

However, in other ways strategic narrative builds upon the failures of soft power. The problem of soft power is that Nye never explains how attraction works in practice. Soft power fails to explain exactly how something becomes attractive, and also how to measure the impact of soft power in terms of changed behavior (Roselle et al, 2014: 74). This lack of

explanation has led to research, which applies soft power on states, to simply count the soft power resources a state has, which Roselle et al (2014: 71-72) consider to be insufficient.

The theory of strategic narrative is more analytically useful because it details how soft power relies on a successful strategic narrative in order to successfully convince other actors of certain values or ideas (Roselle et al, 2014: 74). Roselle et al (2014: 75-76) set out to detail the components of a narrative in order to create a concrete framework in which the specific conditions in which a strategic narrative can be successful is explained. The first component of a strategic narrative is the **actors** that are depicted as having autonomy and being important to the narrative. These can include state actors or non-state actors. The actors are portrayed with certain characteristics or incentives.

The second component is the **setting**, meaning the depiction of the characteristics of the international system that the narrative constructs. For example, if the world is depicted as separated between "us" versus "them" (Roselle et al, 2014: 75-76).

The third component is the depiction of the **conflict**: who is involved and what has happened? The fourth and final component is the **suggested resolution** to the problem, which is a narrative that can limit other actors' actions by setting the limits of what is acceptable behavior (Roselle et al, 2014: 75-76). To study how strategic narratives are formed, one can use textual analyses and interviews (Roselle, 2014: 78).

The intention of this study is to study the American perception of 5G and Huawei, whether it changes or confirms existing conceptions and narratives regarding Chinese influence and technology. The reason why the theory of strategic narrative is relevant for this study is because the aim of the study is to analyze material. As described in the previous section about previous research, there are existing American narratives of China which tend to be negative. Therefore, strategic narrative is a theory that can be considered to be relevant in applying to U.S.-China narratives. Because the relevant material to be analyzed in this study are government-affiliated documents, they can be considered accurate in describing what the prevailing narrative is in the U.S. state apparatus. However, the theory of strategic narrative is also beneficial because it provides guidelines to how the material should be analyzed, which is further explained in the operationalization section of this study.

#### 2.3 Criticism of Strategic Narrative Theory

One point of criticism against strategic narrative theory has been raised by Hagström & Gustafsson (2021) who argue that the theory fails to account for separate narratives that may have an effect on the narrative in focus. They refer to this as "master narratives", defined as narratives that permeate and dominate a discourse which other narratives may then build upon. An example of this would be the master narrative that China is a rising power that needs to be dealt with in some way (2021: 418). Their conclusion is that it's important to account for these narratives, as it could explain why certain narratives might fail or succeed depending on how they align with the master narrative (2021: 435).

Applying the information to this study, it's definitely worth accounting for this master narrative when explaining a Sino-American conflict. There is reason to believe that a master narrative exists in the U.S. regarding China as an antagonizer, considering their troublesome history (U.S. Department of State, 2021). This narrative could be argued to have also affected the narrative surrounding Chinese 5G-technology in the United States.

Another thing to be wary of when conducting a strategic narrative analysis is any potential bias towards ascribing any potential statements by the U.S. government to a specific narrative. What the documents state may not necessarily be proof of the particular strategic narrative between the U.S. and China that this study investigates. Thus, the reproducibility of strategic narrative analyses is questionable, and results may be very indicative and dependent on preconceived notions and narratives by the analysts themselves. This may result in the creation of a narrative about a narrative, when the purpose is merely to document and observe any pre-existing narratives. It's important to be aware of this fact and be as transparent as possible when analyzing the material and thoroughly explain why a statement may or may not be in line with a certain narrative so as to reduce any dissonance between the analyst's conclusions and possible readers (Robertson, 2018: 242-244). This will be taken into account for this analysis.

#### 2.4 Operationalization

To apply the theory to the empirical material gathered, I will use three out of the four components of strategic narrative as the structure of my analysis.

#### 2.4.1 Component one: Actors

Roselle et al (2014: 75-76) describes that relevant autonomous actors are portrayed as having certain characteristics or incentives. This is also called identity narratives, narratives in which the identities of relevant actors are explained (Miskimmon et al, 2013: 7). In this study, the actors in focus are the United States, China and Huawei, as explained by the aim and research question of this study. The empirical material will be analyzed to determine how representations of the strategic narrative of the United States are framing China and of Huawei. This part of the analysis will accordingly focus on two aspects of strategic narratives. The first aspect is which adjectives or words are used to describe the intentions and characteristics of China and Huawei in the material that will be analyzed. This corresponds to Roselle et al's (2014: 75-76) definition of actors being framed as having certain characteristics. Examples include if certain actors are portrayed as undemocratic or unreliable. The second aspect is which goals or incentives China and Huawei are portrayed as having. This is in line with Roselle et al's (2014: 75-76) definition of actors being portrayed as autonomous as well as actors having certain incentives. Examples include if an actor is portrayed as having an explicit goal of spreading their influence.

#### 2.4.2 Component two: setting

As previously explained, the second component of a strategic narrative is the setting, meaning the depiction of the characteristics of the international system that the narrative constructs (Roselle et al, 2014: 75-76). This is what Miskimmon calls the system narratives, which describe the structure of international relations (Miskimmon et al, 2013: 7). In the context of this study, this part of the analysis will focus on how the material, which is written from the United States' point of view, portrays the international system. For instance, the international system can be considered to be viewed as a divisive world if the United States is pushing for other states to also reject Chinese-supplied 5G equipment as that is indicative of a "you're either with us or against us" type of mentality.

#### 2.4.3 Component three: conflict

The third component of strategic narratives is how the conflict is depicted, who is involved and what has happened (Roselle et al, 2014: 75-76). This is also what Miskimmon et al (2013: 7) call the issue narratives, which is defined as the framing of a specific international affair. In the context of this study, the issue or conflict is the framing of Chinese-supplied 5G in the United States. However, as part of the first component of operationalization, the framing of China and Huawei will be a focal point of this study and will already detail U.S. perceptions of security risks associated with Chinese-supplied 5G. Therefore, the framing of the conflict is superfluous as the framing of China and Huawei will already bring up the relevant analysis about the conflict. To avoid unnecessary repetition of analysis, the framing of the conflict will not be brought up in this study.

#### 2.4.4 Component four: suggested resolution

The fourth component is the suggested resolution to the problem, which is a narrative that can limit other actors' behaviors by setting the limits of what is acceptable behavior (Roselle et al, 2014: 75-76). In the context of this study, how China or other actors have responded to the American narrative is not of interest. What is relevant to the research question is which suggested resolutions the United States portrays in the material. That Huawei's operations in the U.S. regarding 5G has been limited through legislation has already been described, however many more suggested resolutions could be described in the material that will be analyzed and it is important to find out what these suggested resolutions are as they give key information about the strategic narrative that the United States is producing. This part of the analysis will detail what specific measures are justified in the four governmental documents with the goal of combating the threat of Chinese-supplied 5G.

#### 3. Method

#### 3.1 Research Design

This study will be conducted as a qualitative case study with a strategic narrative analysis in mind. The benefits of a qualitative study is that it helps to thoroughly go in-depth and explore details about a certain case. Considering that the case is the backbone and focus of this study, a quantitative study wouldn't be as suitable (George & Bennett, 2005: 142). The elements of a specific case can be difficult to quantify and/or compare to other situations in a satisfying manner, which is why a qualitative case study can be better to hone in on the case of interest. The reason why this study will be conducted as a case study is due to the intention of expanding in-depth knowledge about the case of interest, whereas a comparative study would be more suitable to explore a specific aspect of the case and compare it to other cases. The downsides of a comparative study are similar to that of a quantitative study, in that it would hinder the reaching of any deeper conclusions about the specific case of Chinese 5G-technology interests in the U.S (George & Bennett, 2005: 142).

This study will use narrative analysis to analyze and successively reach a conclusion for the research question posed. Narrative analysis allows for less collectivized and less statistically rigid information to be analyzed (Robertson, 2018: 221). A narrative itself can be described as how something is portrayed rather than what it is (Miskimmon et al, 2013: 5). It allows for meaning to be created and attached to otherwise colorless information. Strategic narrative describes the act of attaching a certain meaning to certain information in order to paint a story that can be used to further one's interests (Miskimmon et al., 2013: 5-6). For example, China lends financial aid to African countries, this could be interpreted as simply what has been described. However, when given meaning and context, this action can be weaved into a greater picture of a specific narrative. Chinese politicians could frame the action as showing China's will to help poor states and eliminate poverty and suffering in African countries, while Western politicians could attach far more nefarious meaning to that action, as simply being a smaller part in China's ambitions to spread its harmful influence over the world. By doing so, those who control narratives may also control subsequent reactions by those who are willing to believe the portrayal of that information (Roselle et al., 2014: 71-72). This is precisely what this study is aimed at analyzing. The question then becomes what specific

meaning and context do politicians and other figures of power give to Huawei's potential ambitions in the U.S. ?

Narrative analysis is an important tool for this study, in order to highlight and explain aspects of the wider conflicts of interest between China and the United States. Since bombs are not falling and soldiers are not dying, it would be easy for someone who doesn't read the newspaper to assume that there is no conflict at all. However, when listening in on the interaction between the two states, rhetoric between Chinese state voices versus U.S. state voices make it apparent that the two states are not interacting in a way that two states with cordial relations would interact (Ooi & d'Arcangelis, 2017).

#### 3.2 Material

All primary material that will be used for the analysis consists of documents from the U.S. government. The U.S. National Cyber Strategy (NCS) is a key source of information for this analysis, published during Trump's presidency in 2018 by the White House, being the first of its kind ever published (The White House, 2018).

A National Security Strategy (NSS) document will also be crucial for this study, namely the one published as the Interim National Security Strategic Guidance (INSSG) published in 2021 by the White House (The White House, 2021). President Biden has not yet published an official NSS of his own as of December 2021, this is why any recent developments in the American stance towards Chinese 5G can't be reliably proven or used for this study. This does affect the quality of the analysis, when Biden's stance is not set in stone. It is unlikely however that Biden's presidency would result in a dramatic deviation from the INSSG in tone or narrative towards China and Chinese companies, not only because Biden would appear incredibly inconsistent in his views but also because the narrative of China is something that has largely developed over multiple U.S. presidencies due to the aforementioned path-dependency.

A document from the Congressional Research Service (CRS) will also be used, specifically a study on 5G spearheaded by Jill C. Gallagher and Michael E. DeVine on behalf of the CRS (Gallagher & DeVine, 2019). This document is important because it gives an idea of what

information the United States Congress has to work with, as this study has an entire chapter where Chinese 5G-tech companies are labeled as potential security threats. It is thus reasonable to assume that the information portrayed in this document has in part helped to incorporate companies like Huawei and ZTE who are named directly in this document into a broader narrative of a malevolent Chinese encroachment on the safety of the United States. The document also provides lengthy yet summarized background information on the development and early implementation of 5G-technology, mainly by South Korea, China and the United States.

A document from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) will also be referred to, this document explores the U.S. security aspects of 5G infrastructure in the United States (CISA, 2019). This document also provides important information about what risks will be introduced with 5G adoption in the United States, and also what potential measures should be taken against these security risks.

The reason why these sources are of interest for this analysis is that they represent the official voice and stance of the United States towards China and 5G. While attempting to uncover the narrative aspect of the Sino-American conflicts of interest, it's important to look at how the U.S. portrays China.

To strengthen the analysis, academic studies will also be used. For instance, Friis & Lysne (2021). While outside the realm of strategic narrative theory, their paper provides very useful information about the U.S.' 5G security concerns. This gives an academic take on the American security concerns rather than just the government reports. Roselle et al (2014) and Miskimmon et al (2013) will also be used to describe strategic narrative theory. As these studies are made by experts in their fields or have been peer-reviewed, they are considered reliable sources. In addition to this, other complementary official government sources will also be used. For instance the official U.S. government document establishing Huawei's entity list ban, filed by the Bureau of Industry and Security (2020).

### 4. Analysis

#### 4.1 Actors: How does the U.S. portray China and Huawei?

I will divide this analysis into two parts. First I will analyze how China is portrayed by the material, then Huawei. For each actor, I will begin by analyzing the material in chronological order: the NCS from 2018, the CRS report from 2019, the CISA report from 2019 and finally the INSSG from 2021.

#### 4.1.1 The Portrayal of China

The National Cyber Strategy (NCS) mentions China only two times. In the introduction, different actors that are considered harmful to the U.S. are mentioned, such as China. The document portrays China as conducting cyber espionage and massive intellectual property theft (The White House, 2018: 12). China is mentioned again under the headline of "The Way Forward". It's stated that the Trump Administration engages in a rivalry against adversaries such as Russia, China, Iran and North Korea, all of whom are accused of using cyberspace to challenge the U.S. and its allies (2018: 12). This section continues to describe how China undermines U.S. democracy and economy, and that the U.S. may be a target in cyber attacks orchestrated by the states mentioned (2018: 12-13).

The document frequently refers to "competitors and adversaries" of the U.S. in a negative light. This could be argued to refer to China, as these adversaries are accused of abusing the open internet and violating laws by conducting espionage and cyber attacks, causing economic damage to individuals and governments. It's therefore reasonable to believe that China is mentioned unofficially more than twice (2018: 11).

This negative portrayal of China and attempt to attribute certain characteristics to them aligns with Roselle et al's (2014: 75-76) explanation that strategic narratives involve these types of tendentious descriptions of certain actors. What doesn't fully align with Roselle et al's explanation however, is that the document isn't explicitly mentioning or framing Chinese incentives and ambitions. While it may be understood that the Chinese wrongdoings against the U.S. are attempts to further Chinese interests and their international influence, as long as

it isn't mentioned explicitly it wouldn't be accurate to say that this part of the theory is thoroughly aligning with the document.

In the first page of the CRS report, China is described as a world leader when it comes to the development of 5G alongside South Korea and the United States (Gallagher & DeVine, 2019). One major reason why China is ahead in the development of 5G is because of the government cooperating with private industry to develop the technology, for instance through directly investing \$400 billion in 5G research and development. China is framed as actively wanting to be a world leader in the development of 5G, the CRS report explains that this goal is detailed in China's five-year economic plan (2016-2021). Furthermore, the Chinese government has stated explicit goals of wanting to increase the amount of Chinese components that are in the domestic 5G network, as well as deploy 5G in China in 2020 to increase the competitiveness of Chinese industries as well as to become a "leading supplier of 5G technologies to the world" (Gallagher & DeVine, 2019: 9). According to the CRS report, China has outspent the United States when it comes to 5G infrastructure by \$24 billion as well as having built over ten times as many cell sites (Gallagher & DeVine, 2019: 10). Whether China is ahead of the United States in the development of 5G is debated, and a conclusion has not been reached. The CRS report explains that China's edge in 5G development may threaten the U.S.' competitiveness and free market (Gallagher & DeVine, 2019: 10).

The above parts in the CRS report can be considered to be linked to both aspects of strategic narrative theory. Firstly, the way China is portrayed as a world leader when it comes to 5G development. The CRS report frames China as a very capable actor with power, at least in the realm of technology and 5G. More specifically, because China's technological development in 5G is being compared with the United States', China is being framed as a competitor in the development of 5G, and thus potentially a threat to the United States in the technological realm. As China is being framed as a leader in 5G development and a competitor to the United States, this part of the CRS report is in line with Roselle et al's (2014: 75-76) definition of actors being framed as having certain characteristics. The second aspect is how China is portrayed as having stated goals of wanting to dominate the 5G market. This is in line with Roselle et al's (2014: 75-76) definition of actors being autonomous as well as actors having certain incentives or goals. In this case, China is framed by the CRS report as actively

wanting to become a world leader in 5G development and deployment, not just for domestic means but also to dominate the international market.

The CRS report also details various national security concerns that various security experts and authorities have regarding 5G systems in the United States and how they can be manipulated by foreign actors. For instance, the FBI director Christopher Wray is quoted as saying that some of the risks with 5G include foreign governments gaining the ability to exert pressure over the U.S. telecommunications infrastructure, to be able to steal information or conduct espionage (Gallagher & DeVine, 2019: 28). The FBI Director never specifically mentions China in the CRS report, however the page in which the words appear are in conjunction with a broader discussion of how dangerous China is according to various security experts. On the same page in the CRS document, James Mulvenon, an expert on Chinese cyber issues, is quoted as saying that Chinese laws force Chinese telecommunications operators to provide intelligence to the Chinese state when asked, even when operating in foreign countries, which raises concern about the integrity of data that is connected to the 5G system (Gallagher & DeVine, 2019: 28).

The above paragraph details several characteristics of China that are framed by the CRS report. China is described as being a potential threat to the United States because of the potential to manipulate or steal information. What specific consequences the manipulation or theft of U.S.' data can lead to is not specified. Because the CRS report details that Chinese laws may force Chinese telecommunication corporations abroad to give up information to China, China is not only further framed as a potential threat to U.S. national security, but also framed as having the autonomy and power to force telecommunication companies to give up information even when abroad. However, one vital part of the strategic narrative theory is the explanation of other actors' incentives, and this is lacking in the material as the CRS report does not document any specific incentive for the Chinese government to manipulate the United States' data

The Cybersecurity and Infrastructure Security Agency's (CISA) report titled "Overview of Risks Introduced by 5G Adoption in the United States" only specifically mentions China twice, and never in the context of explaining China's characteristics, incentives or autonomy (CISA, 2019). Consequently, the CISA report can be considered irrelevant for this part of the analysis which specifically focuses on the U.S.' framing of China.

In the Interim National Security Strategic Guidance (INSSG) from March 2021, China is mentioned fifteen times (The White House, 2021). The first sentence in which China is mentioned is the following: "We face a world of rising nationalism, receding democracy, growing rivalry with China, Russia and other authoritarian states, and a technological revolution that is reshaping every aspect of our lives" (The White House, 2021: 6). In the INSSG it is also stated that China is becoming more assertive, and is the sole country "potentially capable of combining its economic, diplomatic, military, and technological power to mount a sustained challenge to a stable and open international system" (The White House, 2021: 8). Furthermore, in the INSSG it is stated that the Chinese government has heavily invested in efforts to combat American interests worldwide (The White House, 2021: 8). It is also stated that the Chinese government uses aggression and coercion in order to obtain unfair advantages, which not only threatens United States' interests worldwide but also undermines the values of an open international system. The rest of the INSSG continues to state that China is assertive, authoritarian, and the number one threat to the United States' interests (The White House, 2021: 20).

The negative framing of China is also contrasted against the positive framing of the United States and American values. For instance, the INSSG states that American companies should not sacrifice American values in doing business in China (The White House, 2021: 21). The United States is explained as being a democratic, diverse and innovative country which is keeping Americans "safe, prosperous, and free", which is a sharp contrast to how China is portrayed as authoritarian (The White House, 2021: 6). However, the INSSG does not state that cooperation with China is impossible. It is explicitly stated that the United States will happily work with China "when it is in our national interest to do so", for instance on issues like climate change and nonproliferation (The White House, 2021: 21).

The above text from the INSSG frames China as having certain characteristics, which connects well to the theory of strategic narratives. China is framed as an authoritarian adversary to the United States', and unique compared to other adversaries such as Russia because of the sheer power and resources that China possesses which means it is the only country that can potentially challenge the openness of the international system. China's government is framed as being aggressive, coercive and not playing by the rules which is framed as threatening to the interests of the United States. Furthermore, U.S. perceptions of

China portray China as the antithesis of the United States, with opposite values compared to the democratic Western state. However, China is still portrayed as an actor that the United States will continue to have some diplomatic relation to, in order to cooperate on specific issues. This indicates that China is framed as very problematic, authoritarian, aggressive but still potentially cooperative in specific scenarios. All of this is in line with Roselle et al's (2014: 75-76) definition of actors being framed as having certain characteristics.

The second aspect of strategic narrative theory, how actors are portrayed as being autonomous and having certain incentives, can also be found in the above text (Roselle et al, 2014: 75-76). The fact that China is described as assertive indicates that the country is framed as having autonomy and incentives. Another indicator of China being framed as having autonomy is that the country is stated to be a potential partner on certain issues. This means the Chinese government is autonomous, and a potentially important partner when it comes to certain issues. This is further underlined when the incentives or goals of the Chinese state are detailed: China's government is stated to have heavily invested in combating American influence worldwide, which means that China is framed as having the explicit goal to limit the spread of American values and influence.

#### 4.1.2 The Portrayal of Huawei

Huawei is never mentioned by name in the NCS, although certain issues are brought up that arguably push a narrative involving Huawei. An instance of this is when former President Trump claims that certain sanctioned malevolent cyber actors aim to conduct harmful cyber activities that requires the U.S. to bolster its protection of networks, systems and data (The White House, 2018: 3). The document also details that the U.S. needs to exclude "risky vendors, products and services" from providing technology for the U.S. government to deploy. It's suggested that the U.S. may have to impose costs and aim to prosecute malicious cyber actors in an effort to deter these actors (The White House, 2018: 16, 19).

The wording of the document would imply that Huawei is targeted here, considering that malicious cyber actors are accused of economic espionage which China is also coincidentally accused of, implying a connection between Huawei and China. The mentioning of cyber actors sanctioned by the U.S. is also compelling evidence that Huawei is described in these

documents, in the light of Huawei's entity list ban (Bureau of Industry and Security, 2020). Huawei has been the biggest target of American discourse regarding implications for U.S. national security if 5G-technology was supplied by foreign actors which would give credence to the claim that this is targeting Huawei (Friis & Lysne, 2021: 1175).

This means that the characteristics that "malicious cyber actors" and "risky vendors" are described as having in the above text can be applied to Huawei. These characteristics that are used to describe Huawei include being an actor which can be exploited by the Chinese state to conduct industrial or economic espionage, to manipulate important data, to undermine American democracy and to conduct cyber attacks. This means that Huawei is framed negatively in the National Cyber Strategy and as a potential threat to the United States' national security. Because Huawei is described with these characteristics, Roselle et al's (2014: 75-76) explanation that actors are framed as having certain characteristics in strategic narratives can be considered to apply to the National Cyber Strategy.

The second aspect of strategic narrative theory, how actors are portrayed as being autonomous and having certain incentives, can partially be found in the above text (Roselle et al, 2014: 75-76). Malicious cyber actors and risky vendors, which has been concluded to refer to Huawei, are described as profiting from malicious cyber activities. This implies that Huawei's incentive is to receive some kind of profit. While the type of profit is not directly stated, it can be guessed that for instance industrial espionage could have aided Huawei in outcompeting other companies in the realm of 5G technology. When it comes to autonomy, however, there are no direct mentions of malicious cyber actors and risky vendors having a choice in the matter. By mentioning the link between malicious cyber actors and China, Huawei is implied to have little autonomy and rather be an extension of the Chinese state. However, as this is not outright stated, the empirical material cannot be claimed to conclusively state anything about Huawei's autonomy.

In the CRS report, national concerns over specific firms such as Huawei are mentioned. It's stated that "some analysts and experts" are concerned about Huawei's influence in the 5G-market and the company's strong ties to the Chinese government (Gallagher & DeVine, 2019: 27). Chinese cyber expert James Mulvenon is quoted as saying that the requirement on Chinese companies to provide information to the Chinese government whenever requested is concerning (2019: 27). FBI Director Christopher Wray details the risks regarding the risk of

letting companies, beholden to governments that do not share U.S. values, to gain access to U.S. telecommunication (2019: 28). An investigation by the House Permanent Select Committee on Intelligence is mentioned as having found such extensive ties between Huawei and China that recommendations were given to limit purchases of American telecommunications companies by Chinese-tied companies. An instance of this was the now-blocked attempt by Broadcom of Singapore to take over the American telecommunications company Qualcomm, the former allegedly having close ties to the Chinese state (2019: 28). It is also mentioned in the CRS report that the heads of federal agencies were prohibited by law from procuring telecommunication equipment from Huawei, due to the Chinese government ties that could pose a U.S. national security risk (2019: 29).

The first aspect of strategic narrative theory, the description of an actor's characteristics, is evident in the CRS report (Roselle et al's (2014: 75-76). Huawei is viewed as a threat, because of the Chinese government's influence over the company which is framed as likely to be used for nefarious purposes due to China's values being opposite to the United States'. This means that Huawei is framed as being a national security threat if allowed to penetrate the U.S. telecommunications market, by giving an entry for the Chinese government to manipulate data and conduct espionage. This is because of the Chinese law which forces Chinese companies to give up information on demand. Huawei is consequently framed very negatively and as an untrusted or dangerous actor, which is why heads of federal agencies are prohibited from using equipment from Huawei and why Huawei would potentially be stopped from merging with other American companies.

The second aspect of strategic narrative theory, how actors are portrayed as being autonomous and having certain incentives, can be partially found in the CRS report (Roselle et al, 2014: 75-76). Huawei is described as being subject to Chinese laws even when abroad. The harm of allowing Huawei to penetrate the U.S. telecommunications market, provide goods and services to heads of federal agencies and to merge with other companies, is framed as concerns that the U.S. has with *every* Chinese telecommunication company. Consequently, the framing of Huawei's characteristics and autonomy is reliant on the framing of China. One research study explains how China has been macrosecuritized by the United States, meaning that anything connected to China is viewed as a threat. In Huawei's case, it has led to the company being portrayed as a possible entryway for Chinese manipulation and espionage rather than the company itself being viewed as inherently threatening (Friis & Lysne, 2021:

1175). This is also what is evident in the CRS report. Because there are no specific mentions of what Huawei's incentives or goals are, this aspect of the strategic narrative theory is unfulfilled.

Huawei is mentioned seven times in the CISA report, for example when it is stated that U.S. federal agencies must not acquire certain equipment and services from Huawei and ZTE (CISA, 2019: 10). The report also mentions the lucrative price range that Huawei and ZTE offers, tempting certain actors to employ these companies. Huawei and ZTE's 4G networks are apparently costly to replace to 5G from other companies, incentivizing actors that have employed Huawei and ZTE to allow them to upgrade their components to 5G-standard to avoid high costs (2019: 11). The report details how 5G components made by untrusted companies can lead to integrity risks, but that a ban of these untrusted companies like Huawei, would risk interoperability difficulties between Chinese 5G-technology deployed abroad and 5G-technology deployed in the U.S. by trusted American companies (2019: 11). The CISA report also mentions that the British National Cyber Security Centre concluded that there are significant issues in "Huawei's approach to software development, which brings significantly increased risk to UK operators" (2019: 11). The first aspect of strategic narrative theory, the description of an actor's characteristics, is evident in the material (Roselle et al, 2014: 75-76). This is because the implication is that Huawei isn't trustworthy, however the document does give room to explanations as to why these Chinese companies have been so successful, thereby posing a bigger threat to U.S. national security since there are great difficulties in stopping these companies.

The second aspect of strategic narrative theory, how actors are portrayed as being autonomous and having certain incentives, cannot be found in the CISA report (Roselle et al, 2014: 75-76). This is because Huawei is not portrayed as having any specific interests or goals, and not portrayed as either having autonomy or not having autonomy.

While the INSSG doesn't specifically mention Huawei, one issue brought up in the document may relate to Huawei. It's stated that the U.S. will confront cyber theft and aim to secure "supply chains for critical national security technologies and medical supplies" (The White House, 2021: 20). Considering the broader accusations of cyber theft and sabotage of critical infrastructure leveled against China by the United States, and that the INSSG report frames China as being hostile (as explained in 4.1.1), it's reasonable to assume that such criticism

refers to actors such as China, through companies like Huawei (Friis & Lysne, 2021: 1175). It's also reasonable to make this claim considering the master narrative of perceiving China in a negative light, with Huawei and other Chinese companies being framed as unsuitable 5G providers due to direct and indirect accusations of cyber theft for instance. This kind of characterization aligns with the first aspect of strategic narrative theory, being indirectly framed as threatening due to the risks of China accessing any data available through Huawei-affiliated 5G networks (Roselle et al, 2014: 75-76).

Regarding the second aspect of strategic narrative theory, Huawei isn't framed as having any incentives nor autonomy (Roselle et al, 2014: 75-76). Huawei is not mentioned, however considering the ties mentioned above, between Huawei and China, any mention of Chinese cyber ambitions is effectively also a reference to Huawei and similar companies and vice versa. Huawei's role as a puppet of the Chinese state seems to be nearly taken for granted, which would imply the complete lack of autonomy of Huawei. This means that the second aspect of strategic narrative theory cannot reasonably be claimed to have been fulfilled.

#### 4.2 Setting: How does the U.S. portray the international system?

The way in which the international system is portrayed in the NCS is noticeably divisive, portrayed as consisting of the free American-led world seeking to spread "universal aspirations for free expression and individual liberty all around the world" that is in conflict with the adversaries to the U.S. (The White House, 2018: 1). The adversaries are defined as having the opposite approach, hindering their own people while standing to benefit from the free world that the U.S. and its allies have created, in order to cause damage. Four countries have been pointed out as adversaries two pages into the document, namely Russia, China, Iran and North Korea (The White House, 2018: 1-2). The document puts the U.S. on a pedestal in the context of the international system, as well as in terms of cyber technology advantages. The document states that adversaries are threatening the U.S.' strong position through underhanded tactics (The White House, 2018: 1-3, 24).

As previously explained, the second component of a strategic narrative is the setting, meaning the depiction of the characteristics of the international system that the narrative constructs. One way the setting can be depicted is as being very divided into two opposing

forces (Roselle et al, 2014: 75-76). The NCS frames the international system as divided into the "good" democratic forces, led by the U.S., and the "bad" autocratic and unjust forces, such as China but also other states. Consequently, the NCS frames the international system as conflicted.

The CRS report describes China, South Korea and the United States as world leaders and competitors in 5G technology. China is described as potentially being able to outcompete the United States in this realm because of China's top-down approach and massive investments into 5G research and development by the Chinese government which are far ahead of the United States' investments into 5G research and development (Gallagher & DeVine, 2019: 10-12). The CRS report also describes that creating international norms and standards is important to ensure security and interoperability, which can promote U.S. technologies and companies abroad (Gallagher & DeVine, 2019: 13-14, 17). The CRS report also details national security concerns with Chinese corporations and Huawei, which are framed as dangerous (Gallagher & DeVine, 2019: 27-30).

The CRS report does contrast the United States and China a lot, but does not portray the entire international system as being divided into two opposing forces. The international setting is not mentioned other than in the context of recommending for the U.S. to stay involved in ensuring international norms in regards to 5G technologies. This can be viewed as positive framing of the international system as the international system is framed as allowing for cooperation between states to ensure security and interoperability.

The CISA report recommends maintaining U.S. membership in certain organizations to ensure universal 5G standards and the promotion of trusted suppliers' interests. The CISA report also states that the use of untrusted 5G equipment should be limited through legislation (CISA, 2019: 12). The CISA report details very little of interest to the framing of the international system. Just like the CRS report, the CISA report states that ensuring international standards of 5G is important. The international system is therefore positively framed as allowing for cooperation between states to ensure security and interoperability. However, the CISA report does state that there are threats that exist in the form of untrusted 5G equipment, but this is not linked to a framing of the international system as no specific actors are mentioned. As this study has previously explained, because of China's macrosecuritization and because of the CISA report framing China in a negative way, these

suggestions may refer to China. In this case, the CISA report only mentions China which is not a framing of the international system but only of a specific actor.

The INSSG describes the setting of the international system as increasingly divisive with authoritarian forces, primarily China but also Russia, Iran and North Korea, rising in power. The INSSG states that the U.S. must fight against these authoritarian forces alongside allies in order to protect American values such as democracy (The White House, 2021: 8, 19). The document emphasizes heavily that there are many global problems that the U.S. necessarily must act upon: "America's fate is inextricably linked to events beyond our shores." (The White House, 2021: 6). From the American perspective, the world is situated at a critical junction where large-scale events, such as the global pandemic and the climate crisis, cannot be ignored if America is to keep Americans "safe, prosperous, and free" (The White House, 2021: 6). In this global struggle between democracy and autocracy, the U.S. very much sees itself as the most important player, stating that "effective global cooperation and institutional reform require America to resume a leadership role in multilateral organizations." and that no greater global threats can be effectively addressed with the U.S. on the sidelines (The White House, 2021: 7, 13). There is a certain balance through the document between addressing domestic and international issues, yet the U.S. appears to perceive the greatest threats coming from abroad, as a reason for its continuous global presence. Therefore, the INSSG can be described as portraying the international system as very problematic, due to the rise of global issues and increasing authoritarianism, and also very divided as the world is framed as black and white: those who are allies to the United States and democracy are framed as good, while adversaries that spread autocracy are bad.

It can be concluded that the NCS and the INSSG frame the international system in a very divided, "good versus evil" way in order to create a strategic narrative trying to convince relevant actors, for instance the American audience and other states, of the moral high ground of the U.S. and the importance of allying against autocratic forces, as well as to discourage autocratic forces from continuing to use underhanded cyber tactics. This is because that is the purpose of strategic narratives: to influence other actors by making more actors accept your framing (Miskimmon et al, 2013: 1-2). Contrastingly, the CRS and CISA reports do frame China as being bad but they do not frame the international system as divisive as they barely bring up other actors. The reports frame the international system as being moldable to the

United States' favor by recommending American membership in organizations with the purpose of creating international 5G standards.

# 4.3 Suggested Resolution: How does the U.S. portray suggested resolutions?

The National Cyber Strategy has several suggested resolutions. Under the headline of "The Way Forward", the Trump Administration details several suggestions in order to protect the United States against malicious cyber activity. The suggested resolutions include continuing to sanction malicious cyber actors, requiring departments to analyze and mend system vulnerabilities and holding department and agency heads accountable for ensuring the safety of cyber systems (The White House, 2018: 12-13). These suggested resolutions are more general and do not specifically mention how to keep the 5G telecommunications network safe, but can be considered to aid in combating future and current threats to the American 5G network. As previously mentioned, Huawei has been placed on the Entity List, and heads of federal agencies are not allowed to use goods and services from Huawei. Therefore, the suggested resolutions above, which are very similar to the current limitations regarding Chinese-affiliated corporations, can be considered to be framed as potentially solving the security issue of Huawei and China dominating the 5G market.

Suggested resolutions with the explicit purpose of protecting 5G networks from malicious actors are also detailed in the NCS. One example includes ensuring that the supply chains of 5G equipment are secure and reliable through excluding risky vendors (The White House, 2018: 16). Because this study has concluded that U.S. perceptions of China and Huawei are overwhelmingly negative as evident in not only the NCS but also the other documents that are analyzed in this study (4.1), and because of the previously explained macrosecuritization of China, this suggested resolution can be considered to directly target Huawei and other Chinese-affiliated actors. This is because Huawei is considered untrusted, because of the connection to the Chinese state, which means the suggested resolution of excluding risky vendors is one way of avoiding this potential risk of Huawei-supplied 5G equipment risking U.S. national security.

Another suggested resolution aimed to protect the American 5G network is that the Trump Administration will "work with the private sector to facilitate the evolution and security of

5G" and "facilitate the accelerated development and rollout of next-generation telecommunications (...) infrastructure here in the United States, while using the buying power of the Federal Government to incentivize the move towards more secure supply chains" (The White House, 2018: 24). Similarly, because of the previously explained framing of China and Huawei as potential threats, and because of the macrosecuritizion of China in American discourse, this suggested resolution is heavily implying that Huawei and other Chinese-affiliated corporations are the untrusted links in the supply chain of 5G equipment that the administration wishes to exclude.

Under the headline of "Policy Considerations for Congress", the CRS report details some suggested resolutions for Congress to consider in order to successfully "address both interest in promoting U.S. competitiveness in the global race to 5G, and an efficient domestic 5G deployment" (Gallagher & DeVine, 2019: 30). These suggested resolutions include imposing "trade restrictions or economic sanctions on foreign technology providers", implementing "policies limiting foreign participation in 5G build-outs", implementing "policies to allocate additional spectrum for future 5G use", "encouraging investment in research and development of new telecommunications technologies" as well as for Congress to consider other policies related to the future use of 5G and IoT devices in order "to ensure security of data" (Gallagher & DeVine, 2019: 31). Because the perception of China as a threat has dominated U.S. security discourse, and because of the previous analysis in this study confirming that China and Huawei are perceived as a threat in the CRS report and the other material, these suggested resolutions that have the aim of ensuring the safety of the 5G network in the United States can be considered to target the threat posed by China and Huawei. These are the actors that the suggested resolutions, such as limiting *foreign* participation in 5G build-outs or imposing trade restrictions of *foreign technology providers*, are aimed at. As previously explained, one fear that the United States has is that China will outcompete American companies. This is one potential outcome that the particular resolution of investing in research and development of new telecommunication technologies aims to avoid.

The CISA report recommends six measures in order for the United States to manage "vulnerabilities and increase the security of communications networks as 5G is adopted" (CISA, 2019: 1). The first of these measures that CISA recommends for the United States' to adopt is to limit the use of untrusted 5G technologies through economic deterrents, and

encourage the use and development of trusted 5G technologies through economic incentives (CISA, 2019: 11). The second measure that CISA recommends is to continue "trusted development of the next generations of communications technologies" by investing and encouraging research and development. This is in order to ensure that the United States can be a world leader when it comes to the development of 6G and in order to lessen reliance on untrusted technologies (CISA, 2019: 11).

The third suggested resolution is for the United States to promote "international standards and processes that are open, transparent and consensus-driven and that do not place trusted companies at a disadvantage" by participating more in organizations that represent telecommunication suppliers' interests (CISA, 2019: 12). The fourth one is limiting the use of vulnerable 5G equipment, and the CISA report brings up the example of federal agencies not being able to use certain equipment and issuing regulations to address the use of telecommunication technology with security risks (CISA, 2019: 12). The fifth recommended measure is for the United States to cooperate with the private sector to identify and mitigate risks within the telecommunication networks (CISA, 2019: 12). The last recommended measure is to "ensure robust security capabilities for 5G applications and services", by expanding risk management to not just protect the 5G infrastructure but also the applications such as IoT devices (CISA, 2019: 12). As has been detailed in this study and in previous research, China and Huawei are perceived as the primary threat to 5G infrastructure according to the United States, which indicates that when these CISA-recommended measures refer to "untrusted technologies", they are actually mostly referring to Chinese 5G technologies such as Huawei's.

The INSSG states that the United States must "reinvigorate and modernize (...) alliances and partnerships around the world" in order to "promote high standards, establish effective international rules, and hold countries like China to account" (The White House, 2021: 10). The INSSG states that in the face of China, the United States should invest in cutting-edge technologies in order to maintain national security in the future. This includes ensuring there's a skilled workforce and that ethical frameworks are established which will regulate how these technologies are used (The White House, 2021: 14). It is also stated that the United States "will double down on science and technology investments to enable the pursuit of numerous national strategic objectives", by investing in research and development of new technologies and ensuring "secure 5G networks" (The White House, 2021: 17). It is also

stated that cybersecurity will be a "top priority", and that it will be achieved through cooperation between the private sector and the government as well as "commitment to international engagement on cyber issues, working alongside our allies and partners to uphold existing and shape new global norms in cyberspace" and holding malicious cyber actors responsible by imposing substantial costs (The White House, 2021: 18). Because the INSSG states that China needs to be held accountable, and that China is a threat to secure 5G networks as a malicious cyber actor, these statements frame China and Huawei as a threat that can be limited or held accountable through adopting these measures.

#### 5. Conclusion

#### 5.1 Answer to Research Question

The research question of this study was the following: How can the US perceptions of Huawei and China, in the context of 5G technology, be explained using the theory of strategic narrative? Through operationalization, the theory of strategic narrative was divided into three sections of analysis: how were the actors China and Huawei framed, how was the international system framed and finally how were the suggested solutions framed by the U.S.?

Regarding the first section of the analysis, the conclusion reached was that U.S. perceptions of China and Huawei are overwhelmingly negative. The NCS, CRS report and the INSSG portray China and Huawei as adversaries, seeking to conduct malicious cyber activity such as espionage. The CISA report makes no relevant mention of China, although Huawei is described as an untrusted company.

Regarding the incentives and autonomy of the actors mentioned, there is variation in how each document portrays it. The NCS only elaborates on Huawei's ambitions to make profit, while emphasizing that Huawei is an extension of the Chinese state and without autonomy. The CRS report also mentions the strong ties between Huawei and China, due to the former's obligation to follow Chinese laws. Huawei's ambitions aren't mentioned, instead, China is seen as an actor seeking to dominate the international 5G-market, unarguably through companies like Huawei. The INSSG also frames Huawei as an extension of Chinese influence, elaborating further on Chinese state ambitions to limit American influence. This document arguably plays in most to the strategic narrative conflict, with China being portrayed as actively trying to limit the U.S. rather than being described as just trying to expand its own influence regardless of the United States. The CISA makes no relevant mention of China or any ties to Huawei. In summary, most sources emphasize the close ties between Huawei and China, effectively saying that Huawei is without autonomy and simply a tool for the Chinese state.

For the second section of the analysis, regarding the framing of the international system, the NCS and the INSSG frame the international system in a very categorical way, being divided into "good versus evil" essentially. It can be argued that this jargon is purposefully inclining any outside actor to take a stance for the morally righteous U.S. against the autocratic rogue states. This is at the heart of strategic narrative, namely to influence actors through acceptance of your framing (Miskimmon et al, 2013: 1-2). In contrast, the CRS and CISA reports did not necessarily attempt to frame the international system in any particular way, as actors other than China were barely mentioned in either of the documents, except for the positive framing of stating that the international system is moldable to the U.S.' favor through joining international organizations with the purpose of creating international 5G standards.

To summarize the framing of the suggested resolutions to the issue of Chinese-supplied 5G, there is strong support for the limiting of Chinese corporate influence on foreign markets. The NCS suggests continued sanctions against malignant cyber actors, such as tech companies associated with China, while also creating a more robust cyber defense against attacks on U.S. state departments and agencies. The CRS report also suggests trade restrictions and sanctions on foreign technology providers, in an attempt to limit foreign participation in 5G-infrastructure installation. The CISA report recommends economic deterrents against "untrusted 5G-technology" and development of trusted 5G-technology

through beneficial economic incentives. The INSSG states that the U.S. must "reinvigorate and modernize (...) alliances and partnerships around the world" in order to establish international rules so that China can be held accountable. The document also mentions that the U.S. will direct efforts to science and technology investments that enable the pursuit of national strategic objectives, without further detail.

As 5G will continue to rise in prominence with time, and in the light of the current U.S.-China tensions, the fact that there were few studies analyzing the American discourse toward Chinese-supplied 5G, and no studies using the theory of strategic narrative was becoming increasingly noticeable and problematic. This study aimed to fill this gap by analyzing U.S.' strategic narrative when it came to Chinese-supplied 5G.

The analysis of American discourse regarding national security could have been done using other theories. One example is securitization theory, which focuses on analyzing speeches and practices in order to determine whether and to what extent an issue is framed as a security issue to a specific audience, e.g. parliament or the broader population (Friis & Lysne, 2021: 1175-1176). One reason why this study does not utilize securitization theory is because one study already exists which focuses on American securitization on Chinese-supplied 5G (see: Friis & Lysne, 2021). Another reason for why securitization theory was not utilized in this study is that securitization theory requires more specification. This study was intended to analyze broader U.S. strategic narratives by choosing four different texts from 2018-2021. National strategies, such as the Trump Administration's National Cyber Strategy and the Biden Administration's Interim National Security Strategic Guidance, can be considered to be political texts intended to inspire confidence in the respective administrations' voter-base. However, the Congressional Research Service report is intended to provide information and recommendations to the Congress, and not intended to reach out to the greater public or society. As the different materials used in this study were intended for different audiences, and by different actors, strategic narrative theory which is more broad and can encompass all of these different texts was deemed to be more fitting.

#### 5.2 Future Research

Future research could further investigate the findings from this study. Since this study's conclusion is that U.S. perceptions of Chinese-supplied 5G are very negative, and that every part of a strategic narrative can be found in the material analyzed in this document, future research can study the effects of this strategic narrative. The goal of strategic narratives is to influence other actors (Miskimmon et al, 2013: 1-2). To study whether the strategic narrative of the U.S. has been effective, future research can attempt to explain how U.S. strategic narratives have helped form anti-Chinese legislation, or other measures created with the purpose of limiting China's influence. Future studies can also attempt to discern whether other state actors have accepted the U.S. discourse on Chinese-supplied 5G, and whether the U.S. has successfully dissuaded allies to not adopt Huawei-technology. Furthermore, future studies can also focus on the American population's perspective on Chinese-supplied 5G and how that has been influenced by the state's strategic narrative, which has also not been a topic of previous research.

#### Reference list

#### **Books**

Miskimmon, A., Roselle, L. & O'Loughlin, B. (2013) *Strategic narratives : communication power and the new world order.* Routledge: London. [Online]

Entman, R. M. (2009) *Projections of Power: Framing News, Public Opinion, and US Foreign Policy.* Chicago: University of Chicago Press. [Online]

George, A. L. & Bennett, A. (2005) *Case studies and theory development in the social sciences.* Cambridge, MIT Press. [Online]

Nye, J. S. (1990) Soft Power. Foreign policy. [Online] (80), 153–171.

Robertson, A. (2018) Narrativanalys. In: Boréus, K. & Bergström, G. *Textens makt och mening*. 4th edition. Studentlitteratur, Lund, pp.219-248.

#### **Digital Articles**

Beckley, M. & Brands, H. (2021) Into the Danger Zone: The Coming Crisis in US-China Relations. *American Enterprise Institute*. [Online] Retrieved: 23/12-21.

https://www.aei.org/research-products/report/into-the-danger-zone-the-coming-crisis-in-us-china-relations/

Breuer, A. & Johnston, A. I. (2019) Memes, narratives and the emergent US-China security dilemma. *Cambridge Review of International Affairs*. [Online] Retrieved 23/12-21. https://par.nsf.gov/servlets/purl/10158389 Bureau of Industry and Security (2020) Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule). *Bureau of Industry and Security*. [Online] Retrieved: 25/12-21.

https://www.federalregister.gov/documents/2020/08/20/2020-18213/addition-of-huawei-non-us-affiliates-to-the-entity-list-the-removal-of-temporary-general-license-and

Chinese National People's Congress (2019) National Intelligence Law of the People's Republic. *28th meeting of the Standing Committee of the 12th National People's Congress*. [Online] Retrieved: 25/12-21.

https://cs.brown.edu/courses/csci1800/sources/2017 PRC NationalIntelligenceLaw.pdf

Cybersecurity and Infrastructure Agency (2020) Overview of Risks Introduced by 5G Adoption in The United States . *Cybersecurity and Infrastructure Agency*. [Online] Retrieved: 30/11-21.

https://www.cisa.gov/sites/default/files/publications/19\_0731\_cisa\_5th-generation-mobile-net works-overview 0.pdf

Federal Bureau of Investigation (n.d.) The China Threat. *Federal Bureau of Investigation*. [Online] Retrieved: 28/11-21.

https://www.fbi.gov/investigate/counterintelligence/the-china-threat

Federal Communications Commission (2020) FCC Designates Huawei and ZTE as National Security Threats. [Online] Retrieved: 29/11-21.

https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats

Figliola, P. M. (2020) TikTok: Technology Overview and Issues. *Congressional Research Service*. [Online] Retrieved: 25/12-21.

https://crsreports.congress.gov/product/pdf/R/R46543

Friis, K. & Lysne, O. (2021) Huawei, 5G and Security: Technological Limitations and Political Responses. *Development and Change (Institute of Social Studies, The Hague)*. [Online] Retrieved: 23/12-21.

https://onlinelibrary.wiley.com/doi/epdf/10.1111/dech.12680

Gallagher, Jill C. & DeVine, Michael E. (2019) Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress. *Congressional Research Service*. [Online] Retrieved: 28/11-21.

https://crsreports.congress.gov/product/pdf/R/R45485

Gomez, G. P., Batalla, G. M., Miche, Y., Holtmanns, S., Mavromoustakis, C. X., Mastorakis, G. & Haider, N. (2021) Security policies definition and enforcement utilizing policy control function framework in 5G. *Computer communications*. [Online] Retrieved: 04/12-21. https://www.sciencedirect.com/science/article/pii/S0140366421001262

Hagström, L. & Gustafsson, K. (2021) The limitations of strategic narratives: The Sino-American struggle over the meaning of COVID-19. *Contemporary security policy*. [Online] Retrieved: 09/12-21.

https://www.tandfonline.com/doi/pdf/10.1080/13523260.2021.1984725

Harold, S. W. & Kamijima-Tsunoda, R. (2021) Winning the 5G Race with China: A U.S.-Japan Strategy to Trip the Competition, Run Faster, and Put the Fix In. *Asia policy*. [Online] Retrieved: 06/12-21.

https://www.nbr.org/publication/winning-the-5g-race-with-china-a-u-s-japan-strategy-to-trip-t he-competition-run-faster-and-put-the-fix-in/

Harrell, P. (2019) 5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation. *Center for a New American Security*. [Online] Retrieved: 04/12-21.

https://www-jstor-org.proxy.annalindhbiblioteket.se/stable/pdf/resrep28738.pdf?refreqid=excelsior%3A574f2aa305c0b76e4b30e11d6c2b78bb

Homolar, A. (2011) Rebels without a conscience: The evolution of the rogue states narrative in US security policy. European journal of international relations. [Online] Retrieved: 18/12-21.

https://journals.sagepub.com/doi/10.1177/1354066110383996

Ji, X., Huang, K., Jin, L., Tang, H., Liu, C., Zhong, Z., You, W., Xu, X., Zhao, H., Wu., J. & Yi, M. (2018) Overview of 5G security technology. *Science China Information Sciences*. [Online] Retrieved: 05/12-21.

https://link.springer.com/article/10.1007/s11432-017-9426-4

Kaska, K., Beckvard, H. & Minárik, T. (2019) Huawei, 5G and China as a Security Threat. *NATO Cooperative Cyber Defence Centre of Excellence*. [Online] Retrieved: 20/12-21. <a href="https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf">https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf</a>

Liu, X. (2020) Chinese Multinational Enterprises Operating in Western Economies: Huawei in the US and the UK. *The Journal of Contemporary China*. [Online] Retrieved: 06/12-21. https://www.tandfonline.com/doi/abs/10.1080/10670564.2020.1827351

Mackinnon, A. (2019) For Africa, Chinese-Built Internet Is Better Than No Internet at All. *Foreign Policy*. [Online] Retrieved: 04/12-21.

https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/

Maizland, L. & Chatzky, Andrew. (2020) Huawei: China's Controversial Tech Giant. *Council on Foreign Relations*. [Online] Retrieved: 04/12-21.

https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant

Ooi, S. M. & D'Arcangelis, G. (2017) Framing China: Discourses of othering in US news and political rhetoric. *Global Media and China*. [Online] Retrieved: 11/12-21. https://journals.sagepub.com/doi/pdf/10.1177/2059436418756096

Roselle, L., Miskimmon, A. & O'Loughlin, B. (2014) Strategic narrative: A new means to understand soft power. *Media, war & conflict*. [Online] Retrieved: 26/11-21. https://journals.sagepub.com/doi/abs/10.1177/1750635213516696 Roslyn Layton & David Witkowski (2021) 5G Versus Wi-Fi: Challenges for Economic, Spectrum, and Security Policy. *Journal of information policy (University Park, Pa.)*. [Online] Retrieved: 04/12-21.

https://www.jstor.org/stable/10.5325/jinfopoli.11.2021.0523#metadata info tab contents

Sacks, D. (2021) China's Huawei Is Winning the 5G Race. Here's What the United States Should Do To Respond. *Council on Foreign Relations*. [Online] Retrieved: 04/12-21. https://www.cfr.org/blog/china-huawei-5g

Salih, A. A., Zeebaree, S. R. M., Abdulraheem, A. S., Zebari, R. R., Sadeeq, M. A. M. & Ahmed, O. M. (2020). Evolution of Mobile Wireless Communication to 5G Revolution. *Technology Reports of Kansai University.* [Online] Retrieved: 04/12-21. https://www.researchgate.net/profile/Mohammed-Msadeeg/publication/342549960 Evolution

of Mobile Wireless Communication to 5G Revolution/links/5efb403c299bf18816f39184

/Evolution-of-Mobile-Wireless-Communication-to-5G-Revolution.pdf

Shafi, M. et al. (2020) A survey on security issues of 5G NR: Perspective of artificial dust and artificial rain. *Journal of network and computer applications*. [Online] Retrieved: 04/12-21.

https://www.researchgate.net/publication/340001347\_A\_survey\_on\_security\_issues\_of\_5G\_NR\_Perspective of artificial dust and artificial rain

Suraci, C., Araniti, G., Abrardo, A. & Bianchi, G. (2021) A stakeholder-oriented security analysis in virtualized 5G cellular networks. *Computer networks (Amsterdam, Netherlands: 1999)*. [Online] Retrieved: 06/12-21.

https://www.researchgate.net/publication/345314523\_A\_Stakeholder-Oriented\_Security\_Analysis in Virtualized 5G Cellular Networks

The White House (2021) Interim National Security Strategic Guidance. *The White House*. [Online] Retrieved: 29/11-21.

https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

The White House (2018) National Cyber Strategy. *The White House*. [Online] Retrieved: 29/11-21.

https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.p

U.S. Department of State (2021) U.S. Relations With China. *U.S. Department of State*. [Online] Retrieved: 09/12-21.

https://www.state.gov/u-s-relations-with-china/

U.S. Executive Order - 13873 (2019) Securing the Information and Communications Technology and Services Supply Chain. *Executive Office of the President*. [Online] Retrieved: 25/12-21.

https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain