



Proceedings of the APAN – Research Workshop 2019
ISBN 978-4-9905448-9-8

Analyzing Cybersecurity-related Articles in Japan's English Language Online Newspapers

Piyush Ghasiya, Koji Okamura

Abstract— Globalization has connected the nations of the world in a way never seen before. Happenings or events in one nation has the potential to impact other nations also. By collecting and analyzing cybersecurity-related articles from three major national newspapers of Japan, this research is trying to find out and understand Japan's newspaper reporting on the cybersecurity issue. Content analysis of those cybersecurity-related articles is used to find critical themes and patterns. The content analysis found that the contention over 5G between the U.S. and China is the most critical issue in Japanese newspapers. From an international relations perspective, the issue between the U.S. and China over 5G is an adverse event represented in newspapers with words such as tussle, tech-war, and contention, but by performing sentiment analysis (content-based analysis) on the articles only related to Huawei, this research tried to find how machine categorize this issue. Then this research critically analyzed the whole 5G war between the U.S. and China and what is Japan's perspective on it.

Index Terms—Content Analysis, Sentiment Analysis, Huawei, 5G, U.S. – China, Newspaper.

I. INTRODUCTION

IN the present time when the news is just a click away, Newspaper has lost its sheen. Gone are the days when people used to wait every morning (sometimes evening also) to get information about the world. Today, 24 hours news channels, social media, and different online platforms are providing happenings of the world instantly. To stay in the race newspapers are also changing their strategy and providing an online version to the audience. Online newspaper in this way is a step ahead from the print edition as along with the trust factor of the print edition; they are just a click away from the audience.

In this scenario, the first step of this research is to collect cybersecurity-related articles for a period of one year from

Piyush Ghasiya, is PhD student at Graduate School of Information Science & Electrical Engineering (ISEE), Kyushu University, Fukuoka, 819-0395 Japan (e-mail: piyushghasiya@gmail.com).

Koji Okamura, is Professor at Research Institute for Information Technology (RIIT), Kyushu University, Fukuoka, 819-0395 Japan (e-mail: oka@ec.kyushu-u.ac.jp).

April 2018 to March 2019 from three of Japan major national newspaper's websites. Python's BeautifulSoup package is used for web-scraping. There is a total of 182 articles. The second step is to perform content analysis to find out what are the main issues of Japan under the cybersecurity field. The content analysis is performed by using KH Coder. The results clearly showed that the U.S. - China contention over 5G is the theme that Japan's newspapers are giving high attention. There are 45 Huawei-related articles which account for 25% of the total corpus. After finding the theme, the third step is to perform the sentiment analysis on the Huawei related articles. For that Python's Textblob package is used. Textblob is one of the best Python libraries to perform sentiment analysis. Sentiment analysis like content analysis is a content-based analysis, unlike critical discourse analysis which focused on context. Though there are methods to finetune the sentiment analysis by using classification methods but for that large amount of data is required. Textblob categorizes 40 articles (89%) into positive. This step shows that the content of Huawei-related articles is positive. It also points towards the limitation of the content-based analysis.

The final fourth step of this research is to critically analyze the U.S. – China tussle over 5G from every possible point of view and tried to give a complete picture. For that first, it is critical to understand what is 5G and its importance. This research further analyzes why Huawei is the center of the technology war between the two most powerful nation in the world. After understanding 5G and Huawei, this research moves towards analyzing the U.S. allegation that Huawei is a national security threat. Lastly, how Japan is dealing with this whole issue, what is at stake for Japan and how policymakers of Japan are looking at this issue.

II. METHODOLOGY & LITERATURE REVIEW

A. Methodology

The first step of this research is to collect the data which in this case is cybersecurity-related articles. By using Python's BeautifulSoup package the English version websites of The Japan Times, Asahi Shimbun, and Mainichi Shimbun was scraped. There is a total of 182 cybersecurity-related articles from April 2018 to March 2019. The next step of this research

is to perform content analysis. Content analysis will be performed by using KH Coder. KH Coder is an open source software for computer-assisted quantitative data analysis mainly quantitative content analysis and text mining [1]. Term frequency analysis and Co-occurrence analysis will be part of content analysis. These analyses will be useful to find out patterns in the collected data. After that sentiment analysis will be performed on the themes that content analysis deemed critical for Japan which in this case is Huawei's 5G issue. For sentiment analysis, Python's TextBlob sentiment analysis package is used. The final step of this research is to analyze the U.S. and China technology war over Huawei's 5G is critical. This step will try to understand how Japan is dealing with this issue and what is at stake for Japan in this tussle.

B. Literature review

Content analysis for International relations (IR) or for newspaper articles is not new. There have been numerous studies in the past that used content analysis as research method. According to Arash Heydarian Pashakhanlao, the first wave of content analysis in lasted from the 1940s to the 1960s. However, after that the discussions regarding the method itself became rare in IR. The advent of new technologies and advancement in information and computer technology renewed interest in the content analysis [2]. In another study Deborah Welch Larson talked about problems of content analysis in foreign policy research way back in 1988 [3].

The content analysis of newspaper articles is becoming popular in present time. C Patterson et al. research utilized content analysis for explaining representation of women's and men's 'binge' drinking in UK newspaper and online news [4]. Similarly, Adem Tasdemir and Zafer Kus also did the content analysis of news in the national papers concerning the renewed primary curriculum [5]. Samantha B. Meyer also used content analysis of newspaper in her research related to the seasonal flu vaccine in Ontario [6].

III. STEP ONE & TWO - DATA ACQUISITION & CONTENT ANALYSIS

A. Step One – Data Acquisition

Cybersecurity-related articles during the past year (from April 2018 to March 2019) from three newspapers- The Japan Times, Asahi Shimbun, and Mainichi Shimbun is used in this research. The Japan Times – 38, Asahi Shimbun – 54, Mainichi Shimbun - 90 articles are collected by using Python's BeautifulSoup package.

TABLE I
NUMBER OF COLLECTED NEWSPAPER ARTICLES

Newspaper	No. of Articles
The Japan Times	38
Asahi Shimbun	54
Mainichi Shimbun	90
Total	182

B. About the Newspapers

1) The Japan Times

The Japan Times is Japan's oldest and largest selling English daily newspaper. It was launched by Motosada Zumoto (editor-in-chief) on March 22, 1897. Headquarter

in Tokyo, the Japan Times has a circulation of around 44,000 copies [7].

2) Asahi Shimbun

Asahi Shimbun is one of the five national newspaper (the other four are: Yomiuri Shimbun, Mainichi Shimbun, Sankei Shimbun and Nikkei Shimbun) in Japan. It began publication on January 25, 1879. As of March 2017, the paper has a circulation of 6.41 million and 2.02 million for morning and evening edition respectively [8].

3) Mainichi Shimbun

As mentioned above, Mainichi Shimbun is one of the five national newspaper in Japan. It started with The Tokyo Nichi Nichi Shimbun on February 21, 1872. Morning and evening edition circulation average around 2.8 million and 720,000 in the first half of 2018 [9].

C. Step Two – Content Analysis

For content analysis, all the articles from each newspaper are considered as a complete text. KH Coder - open source software for computer-assisted quantitative data analysis especially for quantitative content analysis and text mining- is used in this research. Two kinds of analysis- Term Frequency Analysis and Co-occurrence Analysis will be performed on collected articles of each newspaper.

D. Term Frequency Analysis

TABLE II
TOP TEN MOST FREQUENT WORDS IN COLLECTED ARTICLES

The Japan Times		Asahi Shimbun		Mainichi Shimbun	
Word	TF*	Word	TF	Word	TF
huaweus	97	china	207	company	312
u.s.	91	company	200	u.s.	309
government	78	chinese	176	huaweus	277
security	75	huaweus	171	security	219
state	66	government	164	china	213
cybersecurity	63	u.s.	158	government	213
company	58	security	147	trump	206
china	55	state	109	chinese	179
year	55	network	99	year	162
network	53	country	97	network	157

*TF – Term Frequency

Note: 'Huawei's' is written as Huaweus in Table II. It is the peculiarity of KH Coder. It changes the last vowel of noun plural (NNS) part-of-speech tag into 'u'. Though not in Table II but the other example is the word 'data' which is converted into 'datum'.

It is clear from the term frequency analysis that the U.S. - China tussle over Chinese telecom company Huawei's 5G technology was the most prominent theme in Japan's major newspaper under the cybersecurity theme. In all three newspaper words related to this topic acquire a place in the top 10.

E. Co-occurrence Network Analysis

Co-occurrence network is a visualization of the terms that appeared in the studied text together. This analysis not only helps in understanding how the words or themes are connected but also shows which themes are critical. In this visualization, the centrality (or significance) of the word decrease from dark to light color.

For Co-occurrence network, KH Coder provide two options, 1) Subgraph and 2) Centrality. These two categories further divided into three categories. Subgraph have 1) Betweenness 2) Random walks and 3) Modularity. Centrality have 1) Betweenness 2) Degree and 3) Eigenvector. As betweenness centrality shows node's significance as a bridge, for this research, the authors have chosen Betweenness Centrality.

As for extracting co-occurrence network, Noun and Adjective, part-of-speech tags are used.

1) Co-occurrence Network Analysis of The Japan Times

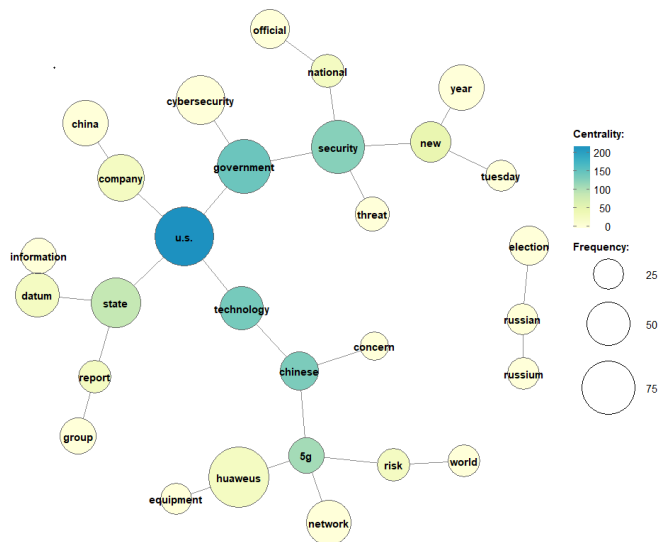


Fig. 1. Co-occurrence Network of The Japan Times Articles (Minimum frequency 20)

Fig. 1. shows that security, government, U.S., technology, Chinese, and 5G are the most critical words in the Japan times cybersecurity-related articles from the past year. It is not difficult to understand the topic they are pointing towards- the US-China tussle over Huawei's 5G technology.

2) Co-occurrence Network Analysis of Asahi Shimbun

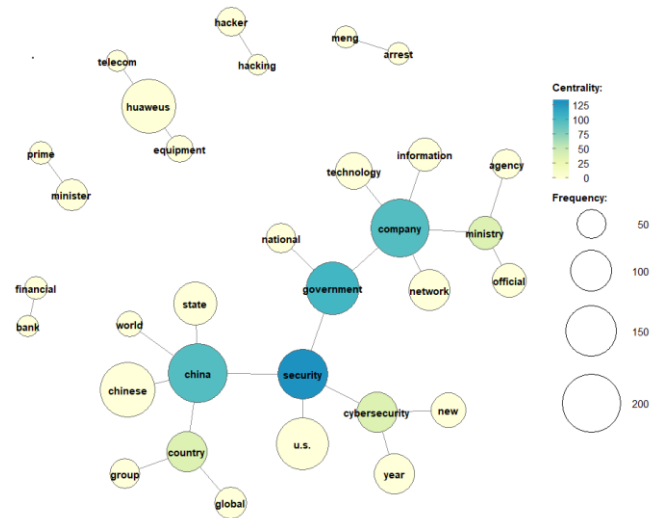


Fig. 2. Co-occurrence Network of Asahi Shimbun articles (Minimum frequency 25)

Fig. 2. shows that China, security, government, and company are the essential words in Asahi Shimbun articles. This figure is also pointing towards the same topic as the Japan Times co-occurrence network has shown - Huawei's 5G technology and the U.S. - China contention.

3) Co-occurrence Network Analysis of Mainichi Shimbun

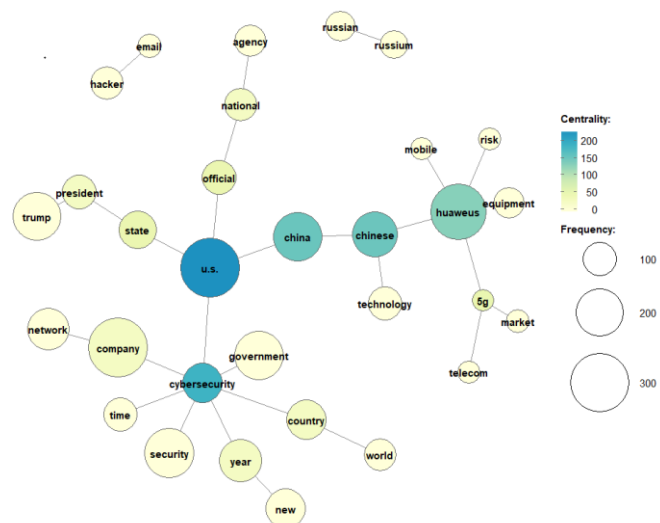


Fig. 3. Co-occurrence Network of Mainichi Shimbun articles (Minimum frequency 40)

According to Fig. 3., cybersecurity, U.S., China, Chinese, and Huawei are the most critical words in Mainichi Shimbun articles, and it is the same as the other two figures -figure 1 and 2 showed. The issue between the U.S. and China over Huawei's 5G technology.

Content analysis (both term frequency analysis and co-occurrence network analysis) point out that in the past one year when it comes to reporting related to cybersecurity, the focus of primary English language national newspapers in Japan was 'the issue between the US and China over Huawei's 5G technology.' The table below shows the number of Huawei-related articles in each newspaper.

TABLE III
HUAWEI-RELATED ARTICLES IN EACH NEWSPAPER

Newspaper	Total No. of Articles	Huawei-related Articles
The Japan Times	38	8
Asahi Shimbun	54	14
Mainichi Shimbun	90	23
Total	182	45

The above table shows that 45 out of 182 articles are Huawei-related. That is 25% of the whole corpus. If one single issue is acquiring a quarter of space under the cybersecurity area, that shows its importance for Japan.

IV. STEP THREE - SENTIMENT ANALYSIS

From the perspective of international relations, the US-China contention over Huawei's 5G technology is a negative issue as many articles use the word tussle, contention, and technology war but do the content of the articles related to this issue also point out towards a negative sentiment? To explore this question, the author performed the sentiment analysis on all the Huawei-related articles.

According to Oxford dictionary, sentiment analysis is the process of computationally identifying and categorizing opinions expressed in a piece of text, especially in order to determine whether the writer's attitude towards a particular topic, product, etc. is positive, negative, or neutral [10].

There are many resources to perform sentiment analysis on the collected text. As mentioned in the methodology, this research used Python's Textblob package for this. Below is the table which shows the sentiment analysis of Huawei-related articles in each newspaper.

TABLE IV
CLASSIFYING HUAWEI-RELATED ARTICLES ACCORDING TO SENTIMENT

Newspaper	Huawei-related Articles	Positive	Negative
The Japan Times	8	7	1
Asahi Shimbun	14	12	2
Mainichi Shimbun	23	21	2
Total	45	40	5

The sentiment analysis categorizes 40 articles (89%) into positive and five articles (11%) into negative.

There are two points which the author would like to point out about the sentiment analysis of these articles.

1) Sentiment analysis is a content-based analysis. Unlike critical discourse analysis where context is essential, sentiment analysis in its basic form does not care about context. There are methods such as classification to finetune the sentiment analysis according to the context, but that can only be done on a vast corpus. For a corpus like this research (only 45 articles), it is not feasible or possible.

2) The second point can be the difference between machine and human understanding. Whereas, human understanding or it would be better to say International relations perspective suggests that the U.S. - China tussle over Huawei's 5G represent the negative sentiment; however, content-based analysis view majority of articles as positive.

V. STEP FOUR - UNDERSTANDING THE U.S. – CHINA CONTENTION OVER HUAWEI'S 5G TECHNOLOGY AND JAPAN'S PERSPECTIVE

There are many factors and different actors involved in this whole issue, and this part will try to understand each of them individually.

A. Why is 5G such a big deal?

In the past century, the world saw a showdown between the two most powerful countries over the dominance of the world. That phase is known as the Cold War, and it was between the U.S. and the Soviet Union. In the present century, the world is again witnessing a similar showdown between two countries for the dominance of the world. This time it is between the U.S. (again) and the People's Republic of China (hereafter China). Ideology (Communist and Capitalist) was the general divider during the Cold War. However, the tussle over 5G has created the same situation as the Cold War.

It is not surprising that the two most powerful countries are fighting over wireless technology because the 21st century is known as the Information Age or Computer age. In this scenario, understanding 5G is significant to understand the whole issue.

In simple term, 5G – G stands for a generation - is the fifth generation of a mobile network. We have seen in the past 1G, 2G, 3G, 4G, and now it is time for 5G. All the previous networks (till 4G) introduced a single feature to the users. 1G – let the mobile talk possible, 2G – let users send text messages, 3G – introduced the internet, and 4G – let users' stream. However, 5G is different; it can not only reach the speed up to 100 times (theoretically) - in current development, the 5G is 20 times faster than the 4G. 4G LTE has a peak speed of 1 GB per second, and 5G has reached 20 GB per second - faster than the 4G networks which remove processing delay, but it will also enable billions of machines, sensors, and appliances at low cost without draining their batteries and in that way kickstarting the internet-of-things revolution [11]. Below are four main features that make 5G so crucial.

1) Bandwidth

Expected to reach up to 1GB per second. A self-driving car generates up to 1 petabyte (1 million GB) data at a time. That makes it clear how significant the higher speed will be for enabling self-driving car and such devices [12].

2) Low Latency-Rate

This feature is one of the essential attributes of 5G. Latency is a delay in the actual processing of the transfer of data. Under the ideal condition, 5G networks are capable of latency rates under one millisecond. That makes 5G, 60 to 120 times faster than then average 4G networks. This feature or advancement enables critical

applications such as remote vehicle control (self-driving car), and Virtual and Augmented reality (VR and AR) which require rapid responsiveness [13].

3) Energy Efficiency

Special focus has been given to make 5G network infrastructure more energy efficient by introducing cloud and virtualization technologies, efficient antenna hardware, 5G small cell network architectures, and more efficient network protocols. These features make 5G to consume less power on devices, that means longer battery life which means less carbon waste [14].

4) Network Capacity

Internet of Things (IoT) that involves connecting billions of devices without human interaction. IoT has the potential to revolutionize the industrial process including business communications, manufacturing, and agriculture. The 5G will work as an enabler for the IoT revolution [15].

B. Importance of 5G from the defense point of view

Along with the traditional domain Land, Air, and Sea, Cyber and Space are termed as the fourth and fifth domain of warfare. In 21st century technology is the enabler for all the domain of warfare. Everything is dependent on technology. At this conjecture, 5G will prove to be a landmark development from a defense perspective. The features mentioned above of 5G will not only bring economic benefits but also take the defense forces to the next level.

According to Dr. Clark She, an AI and telecommunication researcher at the University of Electronic Science and Technology of China, “The 5G network and the internet of things enlarge and deepen the cognition of situations on the battlefield by several orders of magnitude and produce gigantic amounts of data, requiring AI to analyse and even issue commands” [16]. The often-cited scenario given by Liu Zhen of South China Morning Post (SCMP) will help in better understanding the words of Dr. Shu.

“Imagine a group of skirmishers in a jungle. They are moving forward speedily with a distance from one another of a few hundred meters. Each of them wears a wristwatch that displays fellow members’ positions. This is not satellite positioning, because reception in the tropical forest is unstable; it’s machine-to-machine communication.”

“Suddenly one soldier, ambushed by an enemy combatant, is shot and loses consciousness. His smart wearable device detects his condition via sensors, immediately tightens a belt around his wounded thigh, injects an adrenaline shot and sends an emergency alert to the field hospital as well as the entire team.”

“Having received the signal on their wristwatches, the team switch to a coordinated combat formation and encircle the enemy. An ambulance helicopter arrives to evacuate the injured soldier while auto-driven armored vehicles come to reinforce – guided by devices on each soldier and antenna arrays nearby” [16].

Military equipment embedded with communication devices also form the internet of things, and 5G is boon for IoT which makes it revolutionary for defense forces also.

C. Why is Huawei at the center of this 5G tussle?

Huawei was founded in 1987 by Ren Zhengfei and headquartered in Shenzhen, China. Ren Zhengfei served as a military technologist in PLA’s Information Technology Research Unit. He rose to the position of Deputy Director but did not hold military rank and retired in 1983 [17]. According to the company website, it operates in 170 countries with 180,000 employees and 14 R&D centers. Huawei is the world’s second largest manufacturer of smartphones, just behind Samsung. It is the largest telecommunications equipment manufacturer in the world. Huawei provides services in four critical domain- telecom networks, smart devices, IT, and cloud services [18]. Huawei is valued USD 8.4 billion in 2018, and it was the only Chinese company in Forbes’ most valuable brands in 2018 [19].

Since 2009, Huawei is doing R&D in 5G technology, and today it is one of the leaders in 5G technology. In 2017 and 2018, Huawei has invested around USD 1.4 billion in 5G product development. Until March 2019, Huawei had signed 40 commercial deals related to 5G and shipped around 45,000 5G base stations all over the world [20]. According to IPLYtics’s Tim Pohlmann, three points show the progress made by companies in 5G technology. 1) Number of 5G-SEP (5G standard essential patents), 2) Technical contributions towards 5G standards and 3) Attendance of engineers at 5G standards-setting meetings.

1) Number of 5G-SEP (5G standard essential patents)

5G-SEP are the patents that any company will have to use when implementing a standardized 5G technology. 5G-SEP is the best way to understand which companies are leading the 5G patents race. The figure below shows top 5G SEP owners.

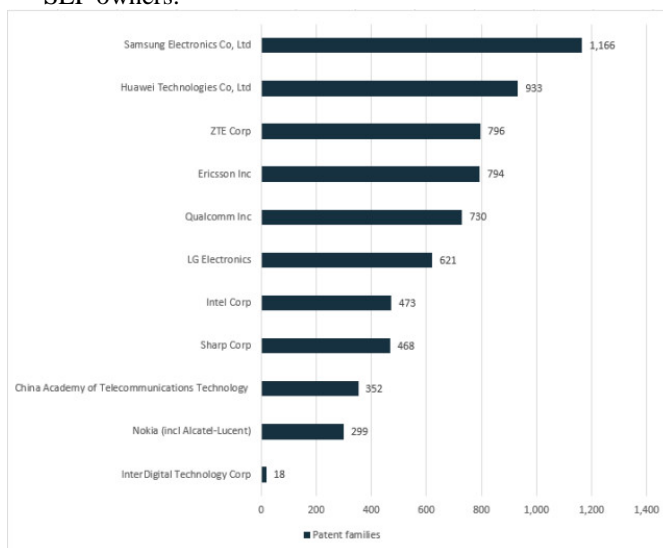


Fig. 4. Top 5G SEP owners [20]

Fig. 4. shows that Huawei is the second leading company just behind South Korea’s Samsung Electronics in 5G patents. These patents will allow their owners to become technology and market leaders by enabling 5G connectivity in various markets. Unlike 3G or 4G technologies which were limited to the telecom sector only, 5G as an enabler of IoT revolution will influence almost every sector whether healthcare, automobile or manufacturing.

2) Technical contributions towards 5G standards

The 5G standards are developed and adapted in international meetings, and companies submit their proposals. Below figure 5 shows technical contribution towards 5G standards by companies.

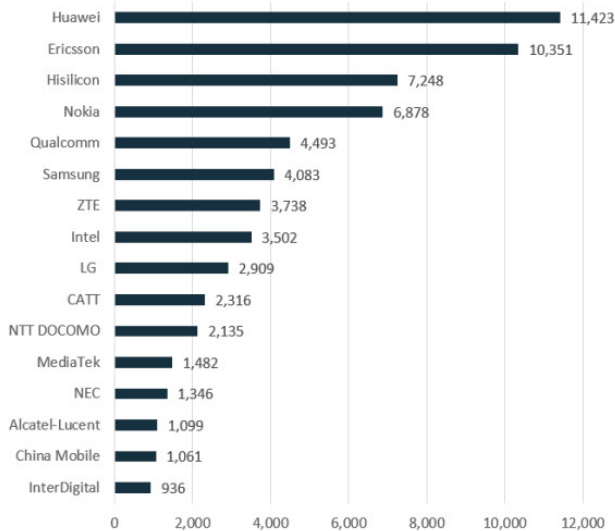


Fig. 5. Companies with the most technical contribution towards 5G standards [20]

It is clear from Fig. 5. that Huawei is leading in technical contribution towards 5G standards. Ericsson- a Swedish company – acquire the second spot in the list. Interestingly, Hisilicon which acquired the third spot in the list is a fabless semiconductor company, and it is a wholly owned subsidiary of Huawei. That makes Huawei by far the most significant contributor of 5G standards.

3) *Attendance of engineers at 5G standards-setting meetings*
 Sending engineers at such meetings is a costly affair both intellectually and financially because these engineers spend time to prepare, travel and discuss technical specifications during these meetings. That reflects a company's willingness to invest in these standards. Below is Fig. 6., showing number of engineers send by companies in 5G standards-setting meetings.

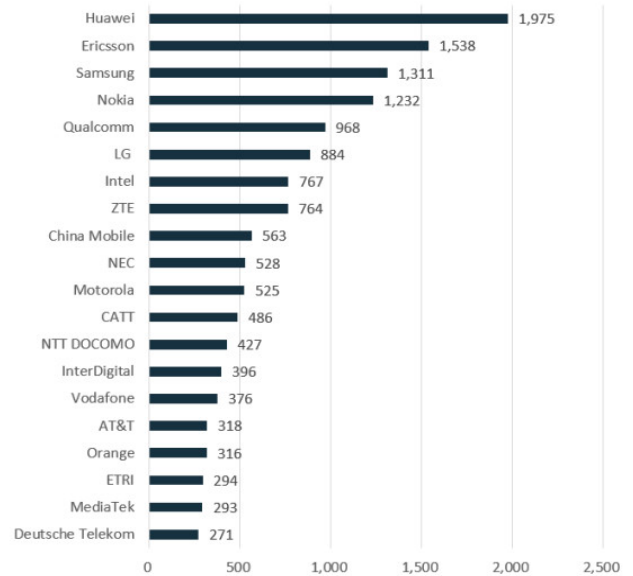


Fig. 6. Attendance at 5G standards-setting meetings [20]

In this list also, Huawei is the top company sending around 2000 engineers in the meetings. Ericsson and Samsung acquired second and third spot respectively.

All three list shows Huawei as a leader, and that shows the when it comes to R&D and investment in 5G technology, Huawei is the undisputed leader.

D. Why Huawei - A National Security Threat to the U.S.

Huawei is involved in several legal battles in many countries since 2001. In June 2003, Cisco sued Huawei for copying source code. Huawei accepted the wrongdoing and agreed to modify its product. However, the major shift came in October 2012 when the U.S. House Intelligence Committee released a report on the national security threat posed by Huawei and ZTE (another Chinese telecom firm). According to this report, a year-long investigation has found that Huawei and ZTE have links with the Chinese government and they have extracted sensitive information from American companies. This report also accused Huawei of not providing complete information about its corporate structure and decision-making process [21]. After this report, the U.S. government banned Huawei from government networks and contracts and later the U.S. carriers and vendors also banned it.

The national security concern once again surfaced in 2018 when Huawei tried to enter the U.S. market this time in consumer electronics - the smartphone. This time heads of six intelligence agencies including FBI, CIA, NSA told the Senate intelligence committee hearing that they advise the U.S. consumers not to use products and services from Chinese firm Huawei [22].

The U.S. companies and government entities have suffered from Chinese cyberintrusions including hackers suspected of working for China's ministry of state security. These past experiences make the U.S. worried about the 'backdoor' that Chinese telecom and computing networks could insert to intercept military, corporate and government communications. However, till now the U.S. has provided no substantial proof the Huawei has done that.

Moreover, the U.S. has also cited China's 2017 National Intelligence Law which requires Chinese companies to support, aid and cooperate in China's national intelligence work, wherever they operate [23]. However, according to an analysis by Nicholas Weaver in Lawfare, telecommunication networks are designed to wiretapping. Communications Assistance for Law Enforcement Act (CALEA) in the U.S. requires that the network operator use equipment that contains surveillance hooks to answer government requests. Similar mandates exist in other countries also [24]. Though the U.S. fear for spying by Huawei is theoretical, the U.S. has done a similar thing to Huawei. According to the leaks by Edward Snowden, as early as 2010 the N.S.A. broke into Huawei's headquarters to prove that the PLA secretly controlled Huawei, but it never found evidence. The operation was code-named 'Shotgiant.' Moreover, the N.S.A. had another goal- to understand Huawei technology and look for potential backdoors. When Huawei would sell these equipment's to the U.S. adversaries, these backdoors would help the N.S.A. to conduct surveillance and if necessary offensive cyberoperations against those U.S. nations [23].

All the facts point out that Huawei is just a pawn in the bigger battle between the two superpowers over the control of future technology. The contention over 5G is a fight for global dominance. The U.S. does not want to lose the position which it has maintained over the past century, and China wants to dethrone the U.S. to become the new hegemon. At present China is winning this race for global dominance.

E. How Japan is dealing with this issue and what is at stake for Japan

The U.S. authority is not stopping to ban Huawei in the U.S. only but spearheaded an aggressive global campaign among its allies to ban Huawei 5G networks and equipment. The U.S. is blackmailing its allies by saying that if they use Huawei 5G, the U.S. will withhold the intelligence [25]. However, the U.S. campaign has failed even among its closest allies. Even some of the Five Eyes – a group of five countries namely the U.S., the U.K. New Zealand, Australia, and Canada which is bound by a joint agreement to share military, human, and signal intelligence are also not heeding to the U.S. pressure. Till now only New Zealand and Australia have banned Huawei 5G, and others are still trying to find a solution to this issue. As Huawei is leading the 5G technology, it would be difficult for countries to ban it from their markets outrightly. Moreover, it will not be feasible from an economic point of view. In this scenario, it would be interesting to understand how Japan - one of the U.S. closest ally in Asia is dealing with this issue.

In early December 2018, the Japanese government proposed new guidelines for procurement of telecom equipment. These new guidelines bar Japan's central government ministries and Self-Defense Forces from buying personal computers, servers, and telecommunications equipment from Huawei and other Chinese companies. These guidelines did not name any specific company [26]. Prime Minister Shinzo Abe in a press conference said that "In order to secure cybersecurity, we are that it is imperative to make sure we would not procure equipment with functions of malicious intention" [27]. That is the first time the Japanese government has compiled procurement guidelines for telecom equipment. This decision

created tension between Japan and China relations which was returning to the normal path after a long time. The Chinese embassy in Japan expressed 'serious concerns' and posted a statement on its website on December 7, 2018. According to this statement, the embassy said that there is no evidence that Huawei and ZTE products have security risks and the ban will raise suspicions that Japan is imposing discriminatory practices against specific companies in specific countries. That created not only a hostile environment for Japan in attracting foreign investment but also for economic cooperation between China and Japan [26].

In April 2019, Japan's regulators allocated the 5G spectrum to four Japanese companies- Softbank, KDDI, NTT Docomo, and Rakuten (new player). These four companies will cumulatively spend around USD 15.29 billion over the five years [28]. As Huawei enjoys the edge in 5G technology, not including it in the Japanese market will compel Japanese telecom companies to spend more. These companies will shift the burden to the consumer by charging high prices for services. According to Zhang Yi of iiMedia Research Institute, a mobile internet consulting firm retaliatory measures towards specific Japanese companies can also be taken not only in 5G but in other sectors also. It will impact Japanese companies very bad as in 2018, Huawei purchased components worth USD 6 billion from Japanese companies [29].

The repercussion will not be limited to 5G or telecom sectors only. Fearing espionage, in June 2018, the U.S. state department shortens the visa period for Chinese students studying subjects such as robotics, aviation and advanced manufacturing from five to one year [30]. If the U.S. would demand similar restrictions from its allies, then it can worsen the dynamics of the overall relationship between China and other countries. This apprehension was stated by Tokyo University professor Yasuhiro Matsuda who is an expert on China-Japan security relations. Speaking at Monash University in Australia, he said that education is the second largest export of Australia with around 200,000 Chinese students studying in Australia in 2018. It would have a massive impact on Australia's economy if the U.S. asked to put similar restrictions on Chinese students [31]. Similarly, Japan also had more than 100,000 Chinese students in 2017, and it will also suffer from the same fate.

Learning from its experience of starting late in 5G related research, Japan and the EU have already started post-5G network research. This research is led by Tetsuya Kawanishi of Waseda University in Tokyo along with Germany's University of Stuttgart, Japan's NEC, Deutsche Telekom and other business, academic, and public entities. This post-5G network will be 1000 times faster than 4G, and the researchers are aiming at the full-fledged introduction of their network in the 2030s. This research is funded by Horizon 2020, the EU's large research and innovation program and Japan's National Institute of Information and Communication Technology [32].

The two superpowers are fighting for the global dominance over 5G in which China is winning. However, the U.S. is still the world leader in the political, military and economic domain which give the U.S. power to negotiate. That is not true for other nations of the world. Most of the nations (even the U.S. also) have a trade deficit with China which gives China the upper hand. Each country should choose whether they want to

ban Huawei or not by carefully examine the U.S. allegations and asking tough questions to Huawei rather than submitting to the pressure of the U.S. Some of the EU nations such as Germany, and the U.K. are defying the U.S. pressure and taking policy decision which reflects their interests. Japan's situation is more complicated than any other nation.

On the one hand, it is dependent on the U.S. for its security as its Article 9 of its constitution does not allow it to have defense forces. On the other hand, Japan is going through the economic recession for a long time and good relations with China (which is growing in a positive direction after a long time) can help its economy in an unprecedented manner. Though Japan took the decision to ban Huawei and visibly irked China, only the future will tell what impact this decision will bring to Japan. As far as 5G is concerned, without Huawei superior and cheaper 5G technology Japanese consumer will surely suffer.

VI. CONCLUSION

As the primary objective of this research is to analyze cybersecurity-related articles in Japan's newspapers by performing the content analysis. The content analysis showed that 25% of all articles are about the U.S. – China contention over Huawei's 5G network. This fact points towards that importance of this issue for Japan.

This research further analyzes this Huawei issue. Therein lies the two sub-objectives of this research. The first sub-objective is to perform sentiment analysis. The U.S. – China is fighting over Huawei's 5G; it is a negative issue from an International relations perspective. However, sentiment analysis categorized 89% of Huawei-related articles into positive. This shows the limitations of the content-based analysis.

Lastly, the second sub-objective is to critically analysis Huawei issue. The talk about Huawei's 5G being a national security threat is concerned, the U.S. has provided no proof whatsoever. In this scenario, each country should work independently to deal with this issue. They can and should talk to Huawei about the cybersecurity of their equipment. If Huawei does not abide by the laws of the country or they found any backdoors in their equipment than they can ban Huawei. However, making decisions due to pressure by the U.S. only shows a country's weakness and policy paralysis. Right now, it is 5G; later it would be something else. China is a challenger to the U.S.'s global dominance, and countries would ask to choose sides just like the Cold war. Choosing a side is not difficult but choosing a side without losing its own space requires a successful diplomatic endeavor, and it is high time that Japan should learn to do that.

VII. FUTURE RESEARCH

The author is planning to collect and analysis cybersecurity-related articles for the same period from the newspapers from countries such as the U.S., the U.K., Canada, Australia, and India. By analyzing newspaper articles from different countries and comparing them can enlighten us about the essential topics under cybersecurity for each country and how similar or different the patterns are between different countries.

REFERENCES

- [1] KH Coder, "About KH Coder," April 2019. [Online]. Available: <http://kxcoder.net/en/>. [Accessed 29 April 2019]
- [2] A. H. Pashakhanlou, "Fully intergrated content analysis in International Relations," *International Relations*, vol. 31, no. 4, pp. 447-465, 2017.
- [3] D. W. Larson, "Problems of Content Analysis in Foreign- Policy Research: Notes from the Study of the Origins of Cold War Belief Systems," *International Studies Quarterly*, vol. 32, no. 2, pp. 241-255, 1988.
- [4] C. Patterson, C. Emslie, O. Mason, G. Fergie, and S. Hilton, "Content analysis of UK newspaper and online news representations of women's and men's 'binge' drinking: a challenge for communicating evidence-based messages about single-episodic drinking?," *BMJ Open*, vol. 6, pp. 1-9, 2016.
- [5] A. Tasdemir and Z. Kus, "The Content Analysis of the News in the National Papers Concerning the Renewed Primary Curriculum," *Educational Sciences: Theory & Practice*, vol. 11, no. 1, pp. 170-177, 2011.
- [6] S. B. Meyer, S. K. Lu, L. Hoffman-Goetz, B. Smale, H. MacDougall and A. R. Pearce, "A Content Analysis of Newspaper Coverage of the Seasonal Flu Vaccine in Ontario, Canada, October 2001 to March 2011," *Journal of Health Communication*, vol. 21, no. 10, pp. 1088-1097, 2016.
- [7] The Japan Times, "The Japan Times Media Information 2017," June 2017. [Online]. Available: https://cdn.japantimes.2xx.jp/wp-content/uploads/2017/08/jt-nyt-media-info_201708_e_small.pdf. [Accessed 23 April 2019].
- [8] Asahi Shimbun, "The Asahi Shimbun- Company Overview 2018," 2018. [Online]. Available: http://www.asahi.com/shimbun/company/csr/eng_overview2018.pdf. [Accessed 23 April 2019].
- [9] Mainichi Shimbun, "Media Data English Version," 2018. [Online]. Available: <http://macs.mainichi.co.jp/english/03.html>. [Accessed 23 April 2019].
- [10] "Oxford Dictionary," 16 April 2019. [Online]. Available: https://en.oxforddictionaries.com/definition/sentiment_analysis. [Accessed 16 April 2019].
- [11] E. Woyke, "China is racing ahead in 5G. Here's what that means.," 18 December 2018. [Online]. Available: <https://www.technologyreview.com/s/612617/china-is-racing-ahead-in-5g-he-res-what-it-means/>. [Accessed 19 April 2019].
- [12] A. Grover, "Everything you need to know about 5G technology (non-technical)," 16 August 2018. [Online]. Available: <https://hackernoon.com/everything-you-need-to-know-about-5g-technology-non-technical-99cb095bde7f>. [Accessed 19 April 2019].
- [13] J. Edwards, "5G versus 4G: How speed, latency and application support differ," 07 January 2019. [Online]. Available: <https://www.networkworld.com/article/3330603/5g-versus-4g-how-speed-latency-and-application-support-differ.html>. [Accessed 25 April 2019].
- [14] R. Keith, "5G ENERGY EFFICIENCY EXPLAINED," 27 March 2019. [Online]. Available: <https://www.a10networks.com/resources/articles/5g-energy-efficiency-explained>. [Accessed 25 April 2019].
- [15] "5G Explained - How 5G works," 25 April 2019. [Online]. Available: <http://www.emfexplained.info/?ID=25916>. [Accessed 25 April 2019].
- [16] L. Zhen, "Why 5G, a battleground for US and China, is also a fight for military supremacy," 31 January 2019. [Online]. Available: <https://www.scmp.com/news/china/military/article/2184493/why-5g-battleground-us-and-china-also-fight-military-supremacy>. [Accessed 25 April 2019].
- [17] "The company that spooked the world," 04 August 2012. [Online]. Available: <https://www.economist.com/briefing/2012/08/04/the-company-that-spooked-the-world>. [Accessed 25 April 2019].
- [18] Huawei, "About Huawei," 25 April 2019. [Online]. Available: <https://www.huawei.com/en/about-huawei/corporate-information>. [Accessed 25 April 2019].
- [19] Huawei Consumer, "Huawei moves up on Forbes Most Valuable Brands of 2018 as China's only company to feature in the global ranking.," 28 May 2018. [Online]. Available: <https://consumer.huawei.com/en/press/news/2018/forbes-most-valuable-brands-2018/>. [Accessed 25 April 2019].

[20] T. Pohlmann, "Who is leading the 5G patent race?," 12 Dec 2018. [Online]. Available: <https://www.iam-media.com/who-leading-5g-patent-race>. [Accessed 26 April 2019].

[21] U.S. House of Representatives, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," 08 October 2012. [Online]. Available: https://fas.org/irp/congress/2012_rpt/huawei.pdf. [Accessed 29 April 2019].

[22] S. Salinas, "Six top US intelligence chiefs caution against buying Huawei phones," 13 February 2018. [Online]. Available: <https://www.cnbc.com/2018/02/13/chinas-huawei-top-us-intelligence-chiefs-caution-americans-away.html>. [Accessed 29 April 2019].

[23] D. E. Sanger, J. E. Barnes, R. Zhong and M. Santora, "In 5G Race With China, U.S. Pushes Allies to Fight Huawei," 26 January 2019. [Online]. Available: <https://www.nytimes.com/2019/01/26/us/politics/huawei-china-us-5g-technology.html>. [Accessed 29 April 2019].

[24] N. Weaver, "A Risk Analysis of Huawei 5G," 17 April 2019. [Online]. Available: <https://www.lawfareblog.com/risk-analysis-huawei-5g>. [Accessed 30 April 2019].

[25] J. E. Barnes and A. Santariano, "U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist," 17 March 2019. [Online]. Available: <https://www.nytimes.com/2019/03/17/us/politics/huawei-ban.html>. [Accessed 30 April 2019].

[26] Nikkei Staff Writers, "Japan bans Huawei and its Chinese peers from government contracts," 10 December 2018. [Online]. Available: <https://asia.nikkei.com/Economy/Trade-war/Japan-bans-Huawei-and-its-Chinese-peers-from-government-contracts>. [Accessed 30 April 2019].

[27] S. Denyer, "Japan effectively bans China's Huawei and ZTE from government contracts, joining U.S.," 10 December 2018. [Online]. Available: https://www.washingtonpost.com/world/asia_pacific/japan-effectively-bans-chinas-huawei-zte-from-government-contracts-joining-us/2018/12/10/748fe98a-fc69-11e8-ba87-8c7facdf6739_story.html?utm_term=.d40fa48ba0c7. [Accessed 30 April 2019].

[28] Reuters, "Japan allocates 5G spectrum with conditions that cement curbs on Chinese vendors such as Huawei," 11 April 2019. [Online]. Available: <https://www.scmp.com/print/tech/policy/article/3005645/japan-allocates-5g-spectrum-conditions-cement-curbs-chinese-vendors>. [Accessed 30 April 2019].

[29] H. Ge, "Japan to lose from ban on Huawei in 5G era," 18 April 2019. [Online]. Available: <http://www.globaltimes.cn/content/1146543.shtml>. [Accessed 30 April 2019].

[30] P. Zengerle and M. Spetalnick, "Exclusive: Fearing espionage, U.S. weighs tighter rules on Chinese students," 29 November 2018. [Online]. Available: <https://www.reuters.com/article/us-usa-china-students-exclusive/exclusive-fearing-espionage-us-weighs-tighter-rules-on-chinese-students-idUSKCN1NY1HE>. [Accessed 30 April 2019].

[31] C. Zappone, "New 'Cold war' could claim Chinese students, says Japanese lecturer," 23 March 2019. [Online]. Available: <https://www.smh.com.au/world/asia/new-cold-war-could-claim-chinese-students-says-japanese-lecturer-20190321-p5163v.html>. [Accessed 30 April 2019].

[32] Z. Yaoyu, "Japan-Europe project to challenge China for post-5G supremacy," 28 March 2019. [Online]. Available: <https://asia.nikkei.com/Spotlight/5G-networks/Japan-Europe-project-to-challenge-China-for-post-5G-supremacy>. [Accessed 30 April 2019].



Piyush GHASIYA was born in Ajmer, (Rajasthan), India in 1985. He received a Master of Arts (M.A.) degree in Japanese Language and Literature from Delhi University in 2012. From 2012 to 2014, he worked as a consultant of the Japanese language in Indira Gandhi National Open University (IGNOU), New Delhi. Then he again moves to pursue higher studies from Jawaharlal Nehru University (JNU), New Delhi. There he completed and received M.Phil. in Japanese Studies in 2016. While pursuing his doctoral studies at JNU, he received the MEXT Scholarship to pursue Doctoral Studies from Kyushu University. Currently, he is a first-year student in a Ph.D. course at Kyushu University, Fukuoka, Japan.

During his master's degree, he worked on Murakami Haruki. His research was on Japan's Whaling issue. He is exploring Japan's cybersecurity from International relations perspective and working on text mining. He is interested in digital humanities especially bringing international relations and computer science together.



Prof. Koji OKAMURA graduated from Graduate School of Computer Science and Communication Engineering from Kyushu University, Japan in 1990. After a short stint in a company in Japan and Graduate School of Information Science, Nara Institute of Science and Technology, Japan and Computer Center, Kobe University, Japan as a Research Associate, he got Ph.D. Degree from Graduate School of Information Science and Electrical Engineering, Kyushu University, Japan in 1998. He worked as an Associate Professor of Computer Center and Graduate School of Information Science and Electrical Engineering, Kyushu University. Since 2011, he has been a Professor of Kyushu University. He is the director of Cybersecurity Center and vice director of Research Institute for Information Technology, Kyushu University. He is vice CISO of Kyushu University.

His current research interests include Cybersecurity for information network and social infrastructure, advanced operation technologies for Internet and Future internets such as Openflow and Virtual Network. He is also researching power-aware and security-aware network operation and developing green power and secure network equipment system. He has contributed introduction of the new technologies into actual campus network of Kyushu University. He has also done many academic case studies using future-oriented Internet and applications for future tele-medical education etc.