A Consideration of the Case Study of Disinformation and its Legal Problems

Tomoko Nagasako[1] [0000-0001-6506-3537]

The Sasakawa Peace Foundation, Tokyo, Japan
t-nagasako@spf.or.jp

Abstract. Recently, some countries deploy global cyberattacks that not only impose destructive measures to the system of industries or infrastructures but also as information warfare, including social networking service (SNS) and other media that affects election results or democratic processes, which becomes a threat to democracy. Thus, this operation is recognized as "disinformation." This paper demonstrates cases of disinformation in cyberspace, and focuses on legal problems in the international law and countermeasures of legal systems in each country.

Consequently, it is found to be challenging to deal with disinformation on the national scale. As there is a limit regarding the regulations by international law, at the present, it is essential to provide the national law about it. I classified the types of countermeasures to find better countermeasures to it based on my considerations, as the number of disinformation cases increased. The regulation for disinformation could violate the freedom of expression and democracy. Therefore, posteriori sanctions against foreign state actors should be applied, and regulations on the contents of media and platformers need to be practiced carefully.

Keywords: Disinformation, Election Meddling, Tallinn Manual, International Law, National Law, Hybrid Warfare.

1 Preamble

Recently, cyber-physical systems are implemented in all areas due to the high growth of information technology. The degree of digitalization and the networking of humans and things are growing rapidly. In modern society, the high added value is found in data accumulation and analysis, which is used in a lot of services. Consequently, a data-driven society is being created; while there is increasing convenience, their risk also increases in parallel, such as information systems being destroyed or compromised, leakage of personal information, unauthorized acquisition and use of intellectual property, and influence operation using social network service (SNS). These changes of risks have also transformed the form of warfare into a new type.

[1] The views expressed in this article are those of the author in my personal capacity.

The cyberspace is recognized as the fifth battlefield, and various cyber tools are incorporated into each country's military strategy. Consequently, the newest warfare shifts from the modern war of using kinetic military weapons to a hybrid war that weaponizes all state activities, including kinetic weapons. There is an increasing sense of crisis in hybrid warfare, that is, it is challenging to draw the line between regular and non-regular battles. In 2017, NATO and the EU established a think tank called "The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Finland. They considered and implemented countermeasures against hybrid threats from various perspectives. The report [1] that Hybrid CoE released in 2018 cites the analysis of the German Marshall Fund's Alliance for Securing Democracy [2] and points out that the Russian government has used cyberattacks, disinformation, and financial influence campaigns to meddle in the internal affairs of at least 27 European and North American countries since 2004. It was pointed out in the previous studies that China has been interfering in domestic affairs through the same operations [3], [4].

Thus, this paper pays attention primarily to disinformation, which hybridizes the tools in Table 1 [5], such as propaganda, fake news, strategic leaks, or organized protest movements.

Table 1. Range of Hybrid Tools

Tools	Salient Points
Propaganda	Enabled and made cheaper by social media, also targeted at home.
Fake news	"Lisa" was portrayed as a Russian-German raped by migrants.
Strategic leaks	Macron emails leaked 48 hours before the election.
Funding organizations	China opened Chinese think-tank in Washington.
Political parties	Russia supports sympathetic European parties on right and left.
Organized protest movements	Russian trolls organized both pro- and anti- protests in Houston mosque case.
"Cyber tools: · Espionage · Attack · Manipulation	New tool in arsenal: espionage is old tactic with new, cyber means. Attack has targeted critical infrastructure, notably in Estonia in 2007. Manipulation is next frontier, changing information without the holders know it.
Economic leverage	China sought to punish South Korea for accepting U.S. anti-missile system.
Proxies and unacknowledged war	Hardly new, but "little green men" in Ukraine slid into actual combat.
Paramilitary organizations	Russian "Night Wolves" bikers intimidate civilians.

Also, an overview of articles about the keyword 'disinformation' from the Journal of Information Warfare [6], a journal closely related to this paper, and reports from US think tank, Atlantic Council [7], shows the current emphasis on Russian operations in North America and Europe. However, as discussed below, in practice, Russia has expanded its activities to Africa and South America, and Chinese disinformation activities are becoming more and more influential in the Asian region. This paper explores these trends through the case study.

Disinformation is a severe challenge to the democracy, since it is executed by combining the leakage of information stolen by cyberattacks with information warfare in media and SNS to transformed public opinion in each country and influence democratic processes, such as elections and demonstrations the outcome. However, planning countermeasures and regulations under national and international cooperation is an urgent issue for disinformation. It is a powerful and complex operation that threatens national sovereignty and sway our democratic system. Hence, it is taken to be one of the new forms of warfare created by the data-driven society that needs to be conquered to ensure a sustainable democracy.

2 What is disinformation?

Since Russia's election meddling[2] in the 2016 US presidential election attracted attention, similar operations by Russia or China emerged. The term of disinformation seems to have become popular. However, some countries use *fake news* in a context similar to disinformation. Though Japan is a representative example of such country, the term *fake news* is not reasonable when discussing foreign influence operations from a national security point of view. *Fake news* is a part of the influence operation, and it does not suit the whole process.

Here, the definition of disinformation should be reconsidered, because more clarifications may be required to make the discussion appropriate.

The European Commission's report [8] calls the situation, including not only influence operations by state actors, but also the dissemination of false information due to negligence, as information disorders, and shows the following three types of data under such circumstances: mis-, dis-, and mal-information. Using the scopes of harm and falseness, it describes the differences between these three types of information (see Fig. 1) as:

- Mis-information is when false information is shared, but no harm is meant.
- Dis-information is when false information is knowingly shared to cause harm.
- Mal-information is when genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere.

The report by the high-level expert group on *fake news* and online disinformation of EU committee [9] also defined *disinformation* as all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit.

[2] Here, I use this word, ‘election meddling’, although some words such as election meddling, election interference or election intervention are used without distinguishing the meanings. This is because the term of intervention is distinguished from the term of interference in international law, and it is hard to distinguish them and to determine which term should be used for each case as following considerations in chapter 4. So I choose ‘election meddling’ without relationship with the argument in international law.

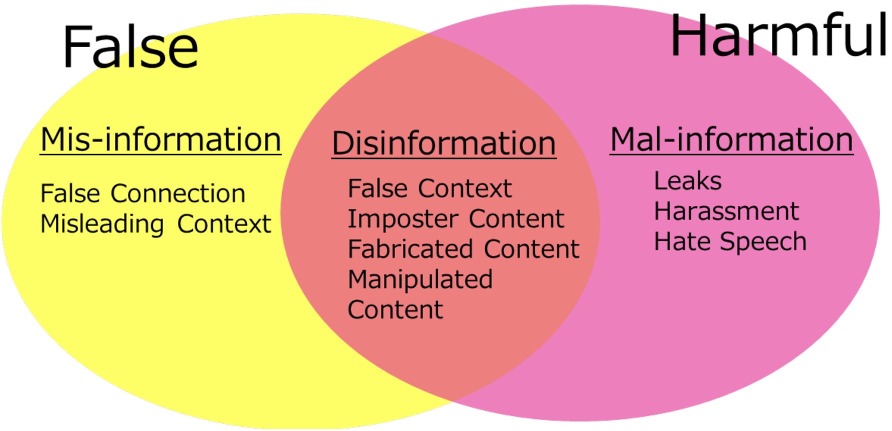

Fig. 1. Definition of Disinformation by EU

However, the definitions are inadequate and seem misleading because they show that disinformation consists of false information only. But disinformation also contains the right information.

For example, in the US presidential election of 2016, the Office of the Director of National Intelligence's report [10] alleges that Russian military intelligence (General Staff Main Intelligence Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release the e-mail data they stole from the Democratic National Committee. This disclosure may have been in a false context, but the data are not wrong.

Also, a specific type of hate speech like in the French presidential election of 2017 has the possibility of truth. In this election period, hate speeches that recognized Macron as a gay with harassment spread widely on some media and SNS [11]. In this case, these were fake news because Macron denied being gay [12] but, if these are true, are these hate speeches not as effective as disinformation? It is immaterial whether it is true or false when an operation uses sensitive information such as religion or sexual orientation. Such a sensitive thing is hard to be fact-checked by a third party, and it is a success for disinformation operation that causes anxiety, confusion, or split in the society to make a social divide wider and damage our democracy. The state actors distort and manipulate the contents of hate speech. So, we should distinguish disinformation that is operated in the frame of the national strategy from ordinary hate speech, and we should exercise caution to correct but harmful information as a part of disinformation.

Fig. 2 shows a modified definition of disinformation. Disinformation contains also true information such as manipulated contents to give a wrong impression or inconvenient truths to harm someone deliberately. If we do not catch the multiple perspectives of disinformation completely, we may not deal with this sophisticated information warfare.

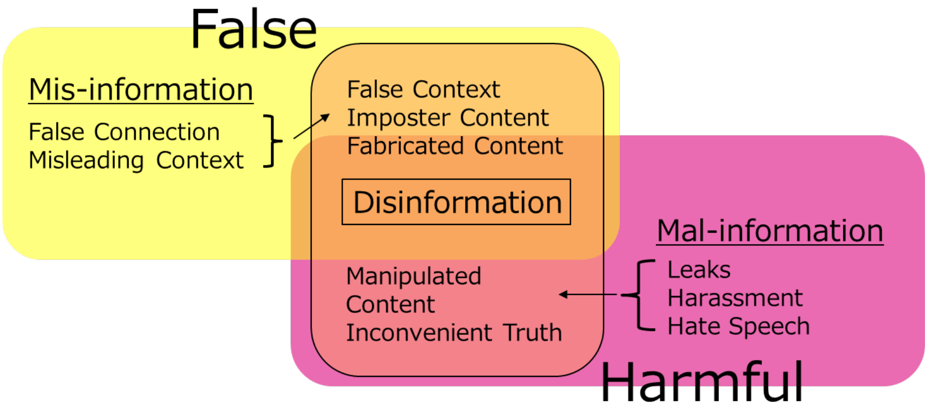

Fig. 2. Definition of Disinformation by the author

3 Disinformation Cases

This chapter shows how much disinformation happen in this world.
As a part of disinformation, the first focus is on election meddling. According to the report [13] of The Canadian Centre for Cyber Security (CCCS), the proportion of national elections in 2018 targeted by foreign cyber threat activity has more than doubled since 2015. As for the Organization for Economic Co-operation and Development countries, the proportion of elections targeted by cyber threat activity is more than 3/4 from 2015 (15.4%) to 2018 (50.0%) [14]. The vast majority (88%) of cyber threat activities affecting democratic processes around the world since 2010 have been strategic (i.e., threat actors specifically targeted a democratic political process to affect the outcome) [15]. Then, the major remainder of the cyber threat activities was cybercrime, which is stealing voter data to sell personal information or use it for criminal purposes. Furthermore, CCCS shows that voters now represent the single largest target of cyber threat activity against democratic processes, accounting for more than half of global activity in 2018 [16]. They explains that this shift seems to have started in 2016, which is likely due to the perceived success among cyber threat actors. Therefore, most foreign adversaries consider the costs and benefits of possible cyber threat activities before undertaking them. They likely recognize targeting voters to be a more effective way to interfere with democratic processes than targeting elections through political parties, candidates, and their staff. The reason is that web media and SNS have made it easier and cheaper to influence the cognitive domain of vast numbers of people.

Figure 3 and Table 2 present the original data of concrete cases of disinformation from 2016. The 2016 example seems to be a turning point because the term of disinformation got more recognized widely after the US presidential election. This data includes not only votes but also some democratic events such as referendums or demonstrations, and it consists of cases I investigated from open sources like government reports and news articles. Though, the CCCS do not make their data available due to security reasons. So, this report is not consistent with the data of CCCS's report.

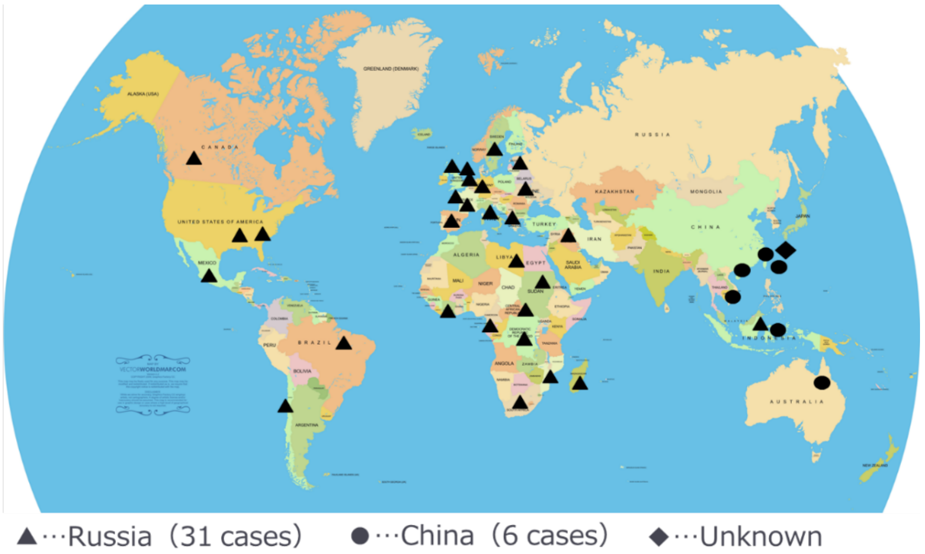

Fig. 3. Disinformation Cases (since 2016)[3]

Table 2. Disinformation cases (since 2016)

2016

	date	Area	Case	Actor
1	2016/1/16	Taiwan	Presidential election and Legislative election	China
2	2016/4/6	The Netherlands	Dutch Ukraine–European Union Association Agreement referendum	Russia
3	2016/6/23	United Kingdom	United Kingdom European Union membership referendum	Russia
4	2016/11/8	United States	Presidential election	Russia

2017

[3] I made this figure thanks to the free map by VECTORWORLDMAP.COM, version 2.2 and COPYRIGHT 2009, Graphics Factory CC.

	date	Area	Case	Actor
1	2017/3/15	The Netherlands	General election (House of Representatives)	Russia
2	2017/5/7	France	Presidential election	Russia
3	2017/9/24	German	Federal election	Russia
4	2017/9/25	Iraq	Kurdistan Region independence referendum	Russia
5	2017/10/1	Spain	Catalan independence referendum	Russia

2018

	date	Area	Case	Actor
1	2018/3/4	Italia	General election	Russia
2	2018/7/1	Mexico	General election	Russia
3	2018/7/29	Cambodia	General election (House of Representatives)	China
4	2018/9/9	Sweden	General election (House of Representatives)	Russia
5	2018/9/30	Macedonia, Greek	Macedonian referendum	Russia
6	2018/9/30	Japan	Okinawa gubernatorial election	Un-known
7	2018/10/7	Brazil	General election	Russia
8	2018/11/6	United States	Midterm election	Russia
9	2018/11/17	France	Yellow vests movement	Russia
10	2018/11/24	Taiwan	Local elections, Kaohsiung mayoral election	China
11	2018/12/19	Madagascar	Presidential election	Russia

2019

	date	Area	Case	Actor
1	～2019/3/4	Estonia, Latvia, Lithuania	Estonian parliamentary election	Russia
2	2019/3/31	Ukraine	Presidential election	Russia
3	2019/3/31～	Hong Kong	Hong Kong protests	China
4	2019/4/17	Indonesia	Presidential election	China, Russia
5	2019/5/8	South Africa	General election (House of Representatives)	Russia
6	2019/5/18	Australia	General election	China
7	2019/5/23-26	EU	Elections to the European Parliament	Russia
8	2019/10/18～	Chile	Chilean protests	Russia
9	2019/10/21	Canada	Federal election	Russia
10	2019/10/30 *	8 African countries	Elections or Political movements	Russia

*This date is not the date of the event but the date when the news that Facebook banned Russian accounts that were related to disinformation operation was reported, because this case expands over some elections and political movements in each county.

2020

	date	Area	Case	Actor
1	2020/1/11	Taiwan	Presidential election and Legislative election	China

The data shows that the area where Russia and China would like to have a strong influence is Europa and Pacific Rim community, respectively. Also, it is manifest that Russia meddles in Africa. These results correspond with their national strategy to expand digital authoritarianism.

Although few cases were investigated, the trends shows that disinformation cases are increasing yearly, which suggests immediate countermeasures against disinformation.

4 Considering the Wrongfulness of Disinformation by International law

As observed earlier, disinformation is a global problem. Since disinformation is a conflict between nations, it may be necessary to consider the unlawfulness of disinformation in the context of international law, and international law should regulate disinformation.

On that note, Tallinn Manual 2.0 [17], which was facilitated and led by the NATO Cooperative Cyber Defence Centre of Excellence, and which summarizes the concept of international law applied to cyber operations is seen. This book does not create new international laws or regulations related to cyberspace and cyber operations. Still, on the assumption that customary international law applicable to cyber operations exists, it confirms and describes 154 rules and its' contents of international law. Here, it is good to consider the unlawfulness of election meddling to be the main operation of disinformation under the related rule of this book.

・Rule 4. – Violation of sovereignty

A state must not conduct cyber operations that violate the sovereignty of another state. [18]

Based on this rule, cyberattacks and cyber espionage conducted by a state organ in the territory of another country are considered a violation of sovereignty. With regard to remote cyber operations, cyberattacks that cause physical damage or loss of functionality in cyberinfrastructure, and cyber operations that interfere with data and services that are necessary to exercise inherently government functions is considered to be a violation of sovereignty, such as changing or deleting data such that it interferes with the delivery of social service, the conduct of elections, the collection of taxes, the effective conduct of diplomacy, and the performance of key national defense activities.

In terms of election interference, it becomes a violation of sovereignty only when there is a level of interference, such as manipulating election voting data through cyberattacks or interfering with the operation of polling stations. So, Information stolen by hacking from election-related organizations and the influence operations using media and SNS will not be considered violation of sovereignty.

・Rule 32. –Peacetime cyber espionage

Although peacetime cyber espionage by states does not per se violate international law, the method by which it is carried out might do so. [19]

This rule is a matter of whether operations such as election meddling constitute unlawful cyber espionage. The operations of disinformation, including election meddling, are so highly compatible with the intelligence agency that at first glance, i.e., the operation itself appears to be included in the cyber espionage. The international hacking groups such as APT28, APT29, and APT40, which are alleged to be involved in election meddling so far, have been pointed out from the attribution results that they have the back of the Russian and Chinese intelligence community such as GRU, FSB, and

Chinese People's Liberation Army, respectively [20], [21], [22]. However, when preventing cyberattacks and cyber espionage, it is necessary to clarify the attribution of the actor conducting the operation, and such activities are similar to normal intelligence activities. Therefore, on the defense side, the intelligence agencies are also involved.

This rule states that the term ‘cyber espionage’ refers to any act undertaken secretly or under false pretenses that uses cyber capabilities to or attempt to, surveil, monitor, capture, exfiltrate, or gather electronically transmitted or stored communications, data, or other information. So, in this context, the rule does not seem to include the covert action to influence or work on another country such as election meddling.

Besides, it should be cautioned that cyber espionage may be conducted in a manner that violates international law due to the fact that certain methods employed to conduct cyber espionage are unlawful. If cyber operations that are undertaken for espionage purposes violate the international human right to privacy, the cyber-espionage operation is unlawful. So, the operation of election meddling is unlawful, if the operation is conducted with, not only an influence operation on SNS but also the cyberattack to steal and leak the e-mails of candidates or election offices, such as in the US and France presidential elections.

・Rule 66. –Intervention by states

A state may not intervene, including by cyber means, in the internal or external affairs of another state. [23]

This manual explains that this rule prohibits coercive intervention, including cyber means, by one state into the internal or external affairs of another. It is based on the international law principle of sovereignty, precisely that aspect of the principle that provides for the sovereign equality of states. In this rule, intervention is clearly distinguished from interference with no coerciveness. For the purpose of this rule, interference refers to acts by states that intrude into affairs reserved to the sovereign prerogative of another country, but lack the requisite coerciveness to rise to the level of intervention. The term of intervention, the subject of this rule, is limited to acts of interference with a sovereign prerogative of another state that have coercive effect. The key is that the coercive act must have the potential for compelling the target state to engage in an action that it would otherwise not take.

So, here, I consider the case of election meddling. Even if disinformation operations are conducted in the media or SNS, as long as various voting possibilities remain, it can be said that it is not unlawful election intervention, but only election interference. It can be recognized as an unlawful election intervention only when a candidate is killed, or the election opportunity itself is lost due to the destruction of the election infrastructure by the attack of another country.

As mentioned above, it seems that there is a limit to identify the wrongfulness of disinformation under current international laws. So, it will be a challenge of future international initiatives to consider what kind of regulation should be taken under international laws from now on, and what type of legislation is useful in the national law of each country.

The G7 “Declaration on Responsible States Behavior in Cyberspace” (i.e., the “Lucca Declaration” [24]) in 2017 expresses their opinion that “We note that, in the interest of conflict prevention and peaceful settlement of disputes, international law also provides a framework for States’ responses to wrongful acts that do not amount to an armed attack - these may include malicious cyber activities. Among other lawful responses, a State that is the victim of an internationally wrongful act may, in certain circumstances, resort to proportionate countermeasures, including measures conducted via ICTs, against the State responsible for the wrongful act in order to cause the responsible State to comply with its international obligations”. It is crucial that they explicitly point out that international wrongful acts include malicious cyber activities. This expression can be recognized as an advanced endeavor to deal with malicious cyber operations that are beyond the scope of existing customary international laws in the framework of new international norms. Such a new movement will have possibilities to create a new framework of international regulations to deterrent disinformation.

A similar international cooperation initiative 'The 'Paris Call for Trust and Security in Cyberspace' was announced by French president Macron at the IGF in 2019. This Paris Call refers to solving problems, such as to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities, and to promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace, and this More than 50 countries and 250 organizations have signed the Paris Call.

However, given the adoption of Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems in 2003, which remains ineffective, any initiatives lack the power to deter their operations without the involvement of Russia and China. The same lack of participation by China and Russia also exists in the G7 and Paris Call, and it is crucial for the formation of new international norms to deter disinformation how these digital authoritarian states are involved.

5 The Types of Countermeasures by the World’s Nations

As seen in the previous chapter, the regulations by international law do not work effectively at present. So, for the time being, we should take countermeasures through national law.

In this section, to the report [25] of the Poynter Institute, that is, a guide for existing attempts to legislate against what can broadly be regarded as online misinformation is referred. At present, they investigated countermeasures of 53 countries and classified their types, focuses, orientations, and details. The authors also recognize the confusing use of the terms of mis- or disinformation, so they seem to choose the term “misinformation” to cover all these concepts, although they do not show and clear the definition in this guide. Then, rearranging these data can show the types of countermeasures. So as to address the problems among the countermeasures, the discussion range is set wider covering all information disorders such as mis-, dis-, mal-information.

Among countermeasures for information disorder, there are 31 of the 53 countries surveyed adopted legal measures such as new legislation and amendments to current laws (see Table 3), which is more than other measures. Additionally, to the measures listed in Table 3, each country has various original measures, such as the establishment of specialized government offices, the creation of a disinformation database, taxation on social media, shutting down the Internet, and making policy recommendations by legislators. Of course, most countries have adopted several measures in multiple layers. However, Table 3 shows that legal regulation is a priority for these countries.

Table 3. Countermeasures for Information Disorder（Top 5 types)

Countermeasures	Contents	Countries
New Law	Regulations by a legislation or a amendment	31
Arrest	Applying existing laws to cases to arrest and charge actors	12
Media Literacy Campaign	Improving the media literacy of voters or the entire nation	11
Task Force	Setting a special team to monitor or investigate suspicious operations	8
Fact Checking	Checking factual information whether it is true or false, and opening the result	8

Therefore, it has classified into the following three types by examining what kind of legal regulation each country enforces: rules on contents of media and platformers, posterior sanctions against foreign state actors, and rules on anti-establishment speeches.

First, the typical examples of regulations on the contents of media and platformers are German and French legislation. In Germany, the Network Enforcement Act (Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, NetzDG) passed in 2017 forces online platforms to remove posts that express obvious illegal contents based on German penal code, including mis-, dis- and mal-information, within 24 hours or face risk fines of €50 million. This Act target social networks with more than 2 million users such as Facebook, YouTube, and Twitter. Furthermore, France passed the law against the manipulation of information (LOI organique n°2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information) in 2018. The law gives authorities the power to remove fake content spread via social media and even block the sites that publish such, as well as enforce more financial transparency for sponsored content, in the three months before an election. This law also provides a definition of "fake news": "Inexact allegations or imputations, or news that falsely report facts, with the intention of changing the genuineness of a vote." It is created to enact strict rules on the media during electoral campaigns and, more specifically, in the three months preceding any election. As for television and radio, if the media that the foreign country has the management rights is reporting fake news, the authorities may order the broadcast to stop. The type of legal regulation on the contents of traditional media or SNS before information disorder, including disinformation spread. However, because of this legal character, this type sometimes is criticized violating freedom of expression.

Second, the typical examples of posteriori sanctions against foreign state actors are American and Taiwanese legislation. In the US, the executive order 13848 (i.e., Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election) was issued in 2018. Thus, within 45 days of the election results, the Director of National Intelligence (DNI) investigated whether there was any election interference, and within another 45 days, the Attorney General and Secretary of Homeland Security to decide whether or not to impose sanctions. It freezes sanctioned persons' assets in the United States and bars them from doing business with Americans. In 2018 midterm election, as a result of the investigation, there was no confirmation of interference with the vote or the alteration of the aggregate results. Moreover, although there was confirmation of influence operations by Russia, China, and Iran, the DNI did not assess the impact on the election results. Taiwan also enacted the anti-infiltration act (反滲透法) in 2020 to prevent foreign hostile forces from interfering to Taiwan. The law prohibits political donations and campaigning for elections under the direction, commission, and financial support of foreign hostile forces, spreading disinformation and obstructing legal demonstrations. This law imposes any miscreant who violates the results five years imprisonment or a fine of five million Taiwanese dollars. It does not regulate the distribution of information because the authorities impose sanctions after the interference of foreign powers is found and upon investigation. Therefore, this type of regulation is considered suitable for the country such as the US or Japan where the right to freedom of expression is paramount, and this type is high possibility that Japan can apply in the legal system from now on. However, it is not easy to operate this regulation because to achieve this, a high attribution ability to identify foreign forces is required.

Finally, the typical example of regulations on anti-establishment speech is the legislation of Russia, China, some other Asians, and African countries. In 2019, Russia passed two legislations banning fake news and disrespect of authorities. One is the Federal Law on Amending Article 15-3 of the Federal Law on Information, Information Technologies and Protection of Information (Федеральный закон от 18.03.2019 № 31-ФЗ "О внесении изменений в статью 15-3 Федерального закона "Об информации, информационных технологиях и о защите информации"), and another one is the Federal Law on Amending the Code of Administrative Violations (Федеральный закон от 18.03.2019 № 27-ФЗ "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях"). Consequently, the dissemination of the wrongful information is banned, such as information that the government has consider to be false; information that is judged to fuel the feelings of hostility, hatred, or malice between groups because of the threat to national security or the threat of public welfare; and false information that may affect the outcome of an election or may undermine the public confidence in the government ability to perform her duties. Platformers are obliged to post corrections and remove content that the government determines to be false, and the government has the authority to order the company to block accounts that spread false information. If the government finds that false information is shared maliciously, the spreader could either face fines of $73,000 or 10 years in prison. As for the amending the code of administrative violations, any act of disseminating information that represents disrespect to Russian society, government, government symbols, constitutions, and ministries is considered illegal. These laws have been criticized against freedom of speech because they stipulate that it is the authority of the government to show that certain information is false or "fake news" under this law, and profane. Similar legislations such as in China, Singapore, and Burkina Faso have also been criticized for the suppression of speech because they have resembled structures that the government, not the judiciary, determines what is illegal information. It is a critical problem to enact the laws that regulate anti-establishment speech in this way on the excuse of countermeasures for information disorder.

As described earlier, this paper classified and argued countermeasures for information disorder. With the current situation in which the definitions of misinformation, disinformation, or fake news are not defined certainly and they are used confusingly, I found it challenging to discuss clearly what the legal regulations are subject to regulation. This paper suggests posteriori sanctions against foreign state actors be considered and applied as the countermeasure for disinformation, because it can focus only on disinformation by state strategy, and it is not related to the aspect of freedom of expression. However, to a certain extent, regulations on contents also are effective to calm down the information disorder including mis-, dis-, and mal-information. Although the situation varies depending on the legal system of the nation, it is necessary to consider the balance between countermeasure for disinformation and freedom of expression in each country.

6 Conclusion

This paper discussed and considered the definition of disinformation, the cases and trends of disinformation, and the countermeasures for disinformation. In general, it is noted that the number of disinformation cases is increasing, and the operations are spreading globally. Moreover, the state actors are shifting the target from the systems or the infrastructures of democratic events such as elections to the voters or the ordinary people. Considering these trends, legal regulations are urgently recommended as the countermeasures to all forms of disinformation. However, since the international law for disinformation is insufficient, many countries ought to cooperate to make the new international norms and rules and the legislations for disinformation. Though, arguments beyond national boundaries are indicated in this critical state to do so. Then, under this situation, it is crucial for the protection of each country's democracy to take the countermeasures by the national law.

Further, although the types of legislation for information disorder are shown, much investigation will be needed to assess which legislation is useful and how it works. However, attention must be paid to avoid allowing the new legislations or countermeasures for disinformation to regulate freedom of expression or participatory democracy. Then, legal issues are forced in this paper, Whereas it is considered crucial to combine various effective countermeasures, such as improving media literacy or fact-checking, in a way that suits each country to establish a democracy based on the human-centric use of data and network. As the environment surrounding disinformation and hybrid war constantly vary in this world, we should continue to make an effort to hold on the situation, investigate, analyze, and cope with this hostile operation exploiting democracy.

Acknowledgement

I am deeply grateful to Prof. Yuasa at Institute of Information Security who offered continuing support and constant encouragement. I am also indebt to Mr. Osawa, Senior Research Fellow at Nakasone Peace Institute who gave me invaluable comments and warm encouragements. Additionally, I would like thank to Enago (www.enago.jp) for the English language review.

References

1. Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue (2018) Addressing Hybrid Threats. Arkitektkopia AB, Bromma.
2. "Alleged Russian political meddling documented in 27 countries since 2004", https://www.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/ (last accessed 2020/2/17).
3. Dean Cheng (2016) Cyber Dragon: Inside China's Information Warfare and Cyber Operations. ABC-CLIO, Westport.
4. Juan Pablo Cardenal et al. (2017) SHARP POWER: Rising Authoritarian Influence. National Endowment for Democracy.
5. Treverton et al. *supra* note 1, p4.
6. DISINFORMATION (key word search): https://www.jinfowar.com/tags/disinformation (last accessed 2020/6/25).
7. Atlantic Council (2016, 2017, 2019) The Kremlin's Trojan Horses 1.0, 2.0, 3.0
8. Claire Wardle, PhD and Hossein Derakhshan (2017) Information Disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe. p5.
9. the independent High level Group on fake news and online disinformation (2018) A multi-dimensional approach to disinformation. European Commission. p5.
10. Office of the Director of National Intelligence (ODNI) (2017) Assessing Russian Activities and Intentions in Recent US Elections. Office of the Director of National Intelligence (ODNI).
11. "Ex-French Economy Minister Macron Could be 'US Agent' Lobbying Banks' Interests," https://sputniknews.com analysis/201702041050340451-macron-us-agent-dhuicq/ (last accessed 2020/2/17).
12. "France election: Macron laughs off gay affair rumours" https://www.bbc.com/news/world-europe-38892409 (last accessed 2020/2/17).

13. The Communications Security Establishment (2019) 2019 UPDATE: CYBER THREATS TO CANADA'S DEMOCRATIC PROCESS. The Communications Security Establishment.
14. *Ibid.*, p16.
15. *Ibid.*, p15.
16. *Ibid.*, p17.
17. Michael N. Schmitt (ed.) and Liis Vihul (ed.) (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge.
18. *Ibid.*, pp17 ff..
19. *Ibid.*, pp168 ff..
20. ODNI, *supra* note7.
21. Estonian Foreign Intelligence Service (2019) INTERNATIONAL SECURITY AND ESTONIA 2019, Estonian Foreign Intelligence Service.
22. "APT40: Examining a China-Nexus Espionage Actor", https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html (last accessed 2020/2/17).
23. Schmitt, supra note14, pp312 ff..
24. G7 DECLARATION ON RESPONSIBLE STATES BEHAVIOR IN CYBERSPACE, https://www.mofa.go.jp/files/000246367.pdf (last accessed 2020/2/17).
25. Daniel Funke and Daniela Flamini, A guide to anti-misinformation actions around the world. https://www.poynter.org/ifcn/anti-misinformation-actions/ (last accessed 2020/2/17).