Int. Cybersecur. Law Rev. (2020) 1:125–136
https://doi.org/10.1365/s43439-020-00010-7

Global disinformation campaigns and legal challenges

Tomoko Nagasako

Received: 7 February 2020 / Accepted: 9 June 2020 / Published online: 6 October 2020

Abstract Recently, some countries have deployed global cyberattacks that not only impose destructive measures on the systems of industries or infrastructures, but also as a type of information warfare, including social networking service (SNS) and other media that affects election results or democratic processes, thereby becoming a threat to democracy. Thus, this kind of operation is recognized as "disinformation." This paper demonstrates cases of disinformation in cyberspace and focuses on legal problems in international laws and countermeasures taken by legal systems in individual countries. Consequently, one finds that it is challenging to deal with disinformation on a national scale. As there is a limit regarding the regulations by international law at present, it is essential to provide national laws for its regulation. Here, the types of countermeasures are classified in order to find improved responses as the number of disinformation cases increases. Since regulations on disinformation could violate freedom of expression and democracy in some cases, subsequent sanctions against foreign state actors should be applied, and regulations on the content of media and online platforms need to be carefully put in place.

Keywords Election meddling · Tallinn Manual · International law · National law · Hybrid warfare

1 Preamble

The degree of digitalization and the information networking of humans and connected devices are growing rapidly. Consequently, the corresponding risks also increase in parallel, such as information systems being destroyed or compromised,

T. Nagasako (✉)
The Sasakawa Peace Foundation, Tokyo, Japan
E-Mail: t-nagasako@spf.or.jp

Table 1 Range of hybrid tools

Tools	Salient points or examples
Propaganda	Enabled and made cheaper by social media, citizens are also targeted even at home by smartphones
Fake news	The "Lisa" case of 2016, where a Russian-German girl was portrayed in the media as being raped by migrants
Strategic leaks	Macron emails leaked 48 h before the election
Funding of organizations	China opened a Chinese think-tank in Washington
Political parties	Russia supports sympathetic European parties on the right and left wing
Organized protest movements	Russian trolls organized both pro- and anti-protests in the Houston mosque case in 2016
Cyber tools Espionage Attack Manipulation	New tool in the arsenal: current espionage is old tactic with new cyber means. Attack has targeted critical infrastructure, notably in Estonia in 2007. Manipulation is the next frontier, changing information without the holder's knowledge
Economic leverage	China sought to punish South Korea for accepting a US anti-missile system
Proxies and unacknowledged war	Hardly new, but "little green men" (masked soldiers of the Russian Federation in unmarked green army uniforms) in Ukraine slid into actual combat
Paramilitary organizations	Russian "Night Wolves" bikers intimidate civilians

(Based on Treverton et al. 2018)

leakage of personal information, unauthorized acquisition and use of intellectual property, and influencing operations using social network services (SNS). These changes to risks have also transformed the current form of warfare into a new type of warfare.

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 only using kinetic military weapons to a hybrid war that weaponizes all state activities. Therefore, there is a growing sense of urgency for hybrid warfare, where the line is very difficult to draw as to whether it is war or not. In 2017, NATO and the EU established a think-tank called "The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)" in Finland. The Hybrid CoE 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 [1, p. 4], such as propaganda, fake news, strategic leaks, or organized protest movements.

Disinformation is a severe challenge to democracy, since it is executed by combining the leakage of information stolen by cyberattacks with information warfare

in media and SNS to transform public opinion in individual countries and to influence democratic processes, such as the outcome of elections and demonstrations. However, planning countermeasures and regulations under national and international cooperation is an urgent issue. Disinformation is a powerful and complex operation that threatens national sovereignty and influences the democratic system. Hence, this new form of warfare created by the information society needs to be defeated so as to ensure sustainable democracy.

2 Interpretation of disinformation

Since Russia's election meddling in the 2016 US presidential election attracted attention, similar operations by Russia or China have emerged. The term 'disinformation' seems to have become popular. However, some countries use *fake news* in a context similar to disinformation. Although Japan is a representative example of such a 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, since more clarification may be required to make the discussion appropriate.

The European Commission's report [5] 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 the European Commission [6] also defined *disinformation* as all forms of false, inaccurate, or misleading information designed, presented, and promoted to intentionally cause public harm or for profit.

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

For example, in the US presidential election of 2016, the report of the Office of the Director of National Intelligence [7] alleges that Russian military intelligence (General Staff Main Intelligence Directorate or GRU) used the hacker group, Guccifer 2.0, persona and the whistleblowing website, DCLeaks.com, to release the email 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 as in the French presidential election of 2017 contains the possibility of truth. In this election period, hate speeches claimed that

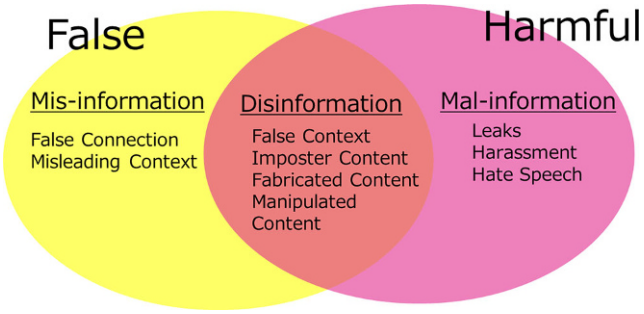

Fig. 1 Definition of disinformation by the European Union

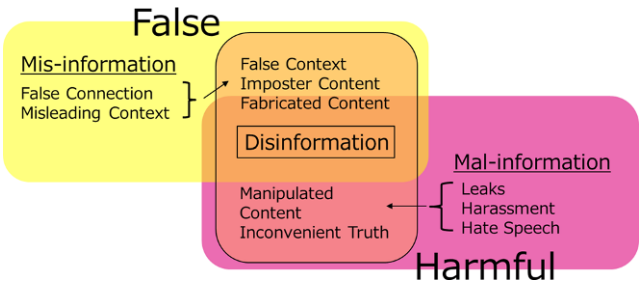

Fig. 2 The author's definition of disinformation

Macron was gay. This harassment was spread widely on some media and SNS [8]. Indeed, in this case, this was fake news as Macron denied being gay [9], but, if true, are these hate speeches not as effective as disinformation? It is not a problem whether it is true or false when an operation uses sensitive information such as religion or sexual orientation. Such a sensitive topic is hard to be fact-checked by a third party, and it is a success for a disinformation operation that causes anxiety, confusion, or discord in the society in order to make a social divide wider and damage democracy. The state actors distort and manipulate the contents of hate speech. Therefore, disinformation that is operated in the framework of the national strategy should be distinguished from ordinary hate speech, and even if it is correct, harmful information should be guarded against.

Fig. 2 shows a modified definition of disinformation. Disinformation also contains true information such as manipulated contents to give a false impression or inconvenient truths to harm someone deliberately. If the multiple perspectives of disinformation are not completely understood, it would be difficult to find appropriate measures for this sophisticated information warfare.

3 Disinformation cases

This article provides a brief overview of worldwide disinformation cases.

With regard to disinformation, the first focus is on election meddling. According to the report [10] 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 has risen more than 75% from 2015 (15.4%) to 2018 (50.0%) [10, p. 16]. 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) [10, p. 15]. Then, the major remainder of 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 [10, p. 17]. They explain 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.

Fig. 3 and Table 2 present the original data of concrete cases of disinformation from 2016. The 2016 example seems to be a turning point, since the term ‘disinformation’ became more widely recognized after the US presidential election. These data include not only votes, but also some democratic events such as referendums or demonstrations, and they consist of cases from open sources such as government reports and news articles.

The data shows that the area where Russia and China would like to have a strong influence is Europe and the Pacific Rim community, respectively. Also, it is manifest

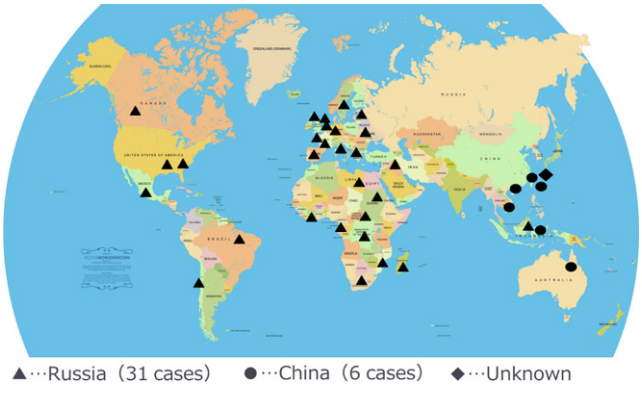

Fig. 3 Disinformation cases (since 2016)

Table 2 Disinformation cases (since 2016)

	Date	Area	Case	Actor
2016				
1	16 January 2016	Taiwan	Presidential election and legislative election	China
2	6 April 2016	The Netherlands	Dutch Ukraine–European Union Association Agreement referendum	Russia
3	23 June 2016	United Kingdom	United Kingdom European Union membership referendum	Russia
4	8 November 2016	United States	Presidential election	Russia
2017				
1	15 March 2017	The Netherlands	General election (House of Representatives)	Russia
2	7 May 2017	France	Presidential election	Russia
3	24 September 2017	Germany	Federal election	Russia
4	25 September 2017	Iraq	Kurdistan Region independence referendum	Russia
5	1 October 2017	Spain	Catalan independence referendum	Russia
2018				
1	4 March 2018	Italy	General election	Russia
2	1 July 2018	Mexico	General election	Russia
3	29 July 2018	Cambodia	General election (House of Representatives)	China
4	9 September 2018	Sweden	General election (House of Representatives)	Russia
5	30 September 2018	Macedonia, Greece	Macedonian referendum	Russia
6	30 September 2018	Japan	Okinawa gubernatorial election	Unknown
7	7 October 2018	Brazil	General election	Russia
8	6 November 2018	United States	Midterm election	Russia
9	17 November 2018	France	Yellow vests movement	Russia
10	24 November 2018	Taiwan	Local elections, Kaohsiung mayoral election	China
11	19 December 2018	Madagascar	Presidential election	Russia
2019				
1	~4 March 2019	Estonia, Latvia, Lithuania	Estonian parliamentary election	Russia
2	31 March 2019	Ukraine	Presidential election	Russia
3	31 March 2019~	Hong Kong	Hong Kong protests	China
4	17 April 2019	Indonesia	Presidential election	China, Russia
5	8 May 2019	South Africa	General election (House of Representatives)	Russia
6	18 May 2019	Australia	General election	China
7	23–26 May 2019	EU	Elections to the European Parliament	Russia

Table 2 (Continued)

	Date	Area	Case	Actor
8	18 October 2019~	Chile	Chilean protests	Russia
9	21 October 2019	Canada	Federal election	Russia
10	30 October 2019[a]	Eight African countries	Elections or political movements	Russia
2020				
1	11 January 2020	Taiwan	Presidential election and legislative election	China

[a]This date is not the date of the event but the date on which the news was reported that Facebook banned Russian accounts that were related to disinformation operations, since this case spans a number of elections and political movements in each county

that Russia meddles in Africa. These results correspond with their national strategy to expand digital authoritarianism.

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

4 Considering the wrongfulness of disinformation cited by customary 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 [11], 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, needs to be considered. This document 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 international rules and their contents of international law. Here, it is helpful to consider the unlawfulness of election meddling to be the main operation of disinformation under the related rule of the Tallinn Manual.

Under international law, the primary issues regarding the wrongfulness of election meddling are whether it constitutes a violation of sovereignty (Rule 4 of Tallinn Manual 20 [11, pp. 17 ff]), whether it constitutes peacetime cyber espionage (Rule 32 [11, p. 168 ff]), and whether it constitutes intervention by the state (Rule 66 [11, p. 312 ff]). The last aspect in particular will be examined, since the main focus of election meddling is the conduct of this operation to be considered as intervention.

Rule 66, "Intervention by states," states that a state may not intervene, including by cyber means, in the internal or external affairs of another state.

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 for 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 in a sovereign prerogative of another state that have a coercive effect. The key is that the coercive act must have the potential to compel the target state to engage in an action that it would otherwise not take.

Thus, the case of election meddling is considered here. 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 identifying the wrongfulness of disinformation under current international laws. Therefore, 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 laws of individual countries.

The G7 "Declaration on Responsible States Behavior in Cyberspace" (i.e., the "Lucca Declaration" [12]) of 2017 expresses the following opinion: "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 statement 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 deter disinformation.

5 Types of countermeasures against disinformation taken by the world's nations

As mentioned above, the by international legal regulations do not work effectively at present. Therefore, for the time being, countermeasures through national law should be taken into account.

This section refers to the report of the Poynter Institute, "A guide to anti-misinformation actions around the world" [13], which is a guide for existing attempts to legislate against what can broadly be regarded as online misinformation. At present,

Table 3 Countermeasures to information disorder (top five types)

Countermeasures	Contents	Countries
New law of misinformation, disinformation, or fake news	Regulations by means of legislation or an 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 whether factual information is true or false, and releasing the result	8

countermeasures of 53 countries have been investigated and classified according to type, focus, orientation, and details. The authors of the report also recognize the confusing use of the terms mis- or disinformation, so they seem to choose the term "misinformation" to cover all these concepts, although they do not show and clarify the definition in this guide. Therefore, these data need to be rearranged so as to show the types of countermeasures. In order to address the problems with countermeasures, the discussion range is set wider, covering all information disorders such as mis-, dis-, and mal-information.

Among countermeasures for information disorder, 31 of the 53 countries surveyed adopted legal measures such as new legislation and amendments to current laws (see Table 3). In addition to the measures listed in Table 3, each country has various unique 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.

These countermeasures are then classified into the following three types by examining what kind of legal regulation each country enforces: rules on content of media and platforms, subsequent sanctions against foreign state actors, and rules on anti-establishment speeches.

First, the typical examples of regulations on the content of media and platforms are found in 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 h or risk fines of €50 million. This act targets social networks with more than two 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 content, 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 was 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 for which the foreign country has the management rights is reporting fake news, the authorities may order the broadcast to stop. The legal regulation of the content of traditional media or SNS in terms of information disorder, including disinformation, is becoming increasingly common. However, due to its legal character, this type of regulation is sometimes criticized for violating freedom of expression.

Second, the typical examples of subsequent sanctions against foreign state actors are American and Taiwanese legislation. In the US, the executive order 13,848 (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 had to decide whether or not to impose sanctions, which would have frozen sanctioned persons' assets in the United States and barred them from doing business with American citizens. In the 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 a 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 in Taiwan. The law prohibits political donations and campaigning for elections under the direction, commission, and financial support of foreign hostile forces, thereby spreading disinformation and obstructing legal demonstrations. This law imposes five-year imprisonment or a fine of five million Taiwanese dollars on any miscreant who violates the results. It does not regulate the distribution of information since the authorities impose sanctions after the interference of foreign powers is found and upon investigation. Therefore, this type of regulation is considered suitable for countries such as the US or Japan where the right to freedom of expression is paramount, and this type of regulation has a good chance of being adopted in the Japanese legal system from now on. However, it is not easy to operate this regulation since, to achieve this, a strong ability to identify and attribute the activity to foreign forces is required.

Finally, the typical example of regulations on anti-establishment speech is the legislation of Russia, China, a number of other Asian countries, and African countries. In 2019, Russia passed two pieces of legislation 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 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 wrongful information, such as information that the government has deemed to be false, is banned,; information that is judged to fuel feelings of hostility, hatred, or malice between groups due to the threat to national security or the threat of

public welfare; and false information that may affect the outcome of an election or undermine public confidence in the government's ability to perform its 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 face either fines of $73,000 or 10 years in prison. As for the amendment of 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 as breaching freedom of speech, since they stipulate that it is the authority of the government to show that certain information is false or "fake news" under this law, and thus profane. Similar pieces of legislation in, e.g., China, Singapore, and Burkina Faso have also been criticized for suppressing speech since they resemble structures that the government, not the judiciary, determines to be illegal information. Enacting laws that regulate anti-establishment speech in this way on the premise of countermeasures to information disorder is a crucial problem.

As described earlier, this article classifies and discusses countermeasures for information disorder. The article suggests subsequent sanctions against foreign state actors that should be applied as countermeasures to disinformation, since it can focus only on disinformation by state strategy and is not related to the aspect of freedom of expression. However, to a certain extent, regulations on content are also effective to ease 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 a countermeasure for disinformation and the freedom of expression in the individual countries.

6 Conclusion

This article discusses and considers the definition of disinformation, the cases and trends of disinformation, and the countermeasures to 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 countermeasures to all forms of disinformation. However, since the international law on disinformation is insufficient, many countries ought to cooperate to create new international norms and rules as well as legislation against disinformation. However, to this end, discussions beyond national boundaries is indicated in this critical state. Therefore, in this situation, it is crucial for the protection of each country's democracy to take countermeasures in the form of national legislation.

Furthermore, although the types of legislation on 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 new pieces of legislation or countermeasures to disinformation to regulate freedom of expression or partici-

patory democracy. Thus, legal issues are mainly argued in this paper, whereby it is considered crucial to combine various effective countermeasures, such as improving media literacy or fact-checking, in a way that suits each country in order 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 today's world, one needs to continue making an effort to keep a hold on the situation, as well as investigate, analyze, and cope with these hostile operations exploiting democracy.

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

References

1. Treverton GF, Thvedt A, Chen AR, Lee K, McCue M (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/. Accessed 17 February 2020
3. Cheng D (2016) Cyber dragon: inside China's information warfare and cyber operations. ABC-CLIO, Westport
4. Cardenal JP et al (2017) SHARP POWER: rising authoritarian influence. National endowment for democracy
5. Wardle C, Hossein Derakhshan (2017) Information disorder: toward an interdisciplinary framework for research and policymaking. Council of Europe, Strasbourg Cedex, p5.
6. The independent High level Group on fake news and online disinformation (2018) A multi-dimensional approach to disinformation. European Commission, Luxembourg, p5.
7. "Assessing Russian activities and intentions in recent US elections." Office of the Director of National Intelligence (ODNI)(2017). https://www.dni.gov/files/documents/ICA_2017_01.pdf. Accessed 17 February 2020
8. "Ex-French Economy Minister Macron Could be 'US Agent' Lobbying Banks' Interests,". https://sputniknews.com/analysis/201702041050340451-macron-us-agent-dhuicq/. Accessed 17 February 2020
9. "France election: Macron laughs off gay affair rumours" https://www.bbc.com/news/world-europe-38892409. Accessed 17 February 2020
10. "2019 update: Cyber threats to Canada's democratic process", The Communications Security Establishment (2019). https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf. Accessed 17 February 2020
11. Schmitt MN, Vihul L (eds) (2017) Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, Cambridge
12. G7 Declaration on responsible state behaviour in cyberspace, https://www.mofa.go.jp/files/000246367.pdf. Accessed 17 February 2020
13. Funke D, Flamini D (2020) A guide to anti-misinformation actions around the world. https://www.poynter.org/ifcn/anti-misinformation-actions/. Accessed 17 Feb 2020