博士論文

Global Disinformation Campaigns and Strategic Challenges -Case Study and Consideration of National Strategies as the Countermeasures–

Tomoko NAGASAKO

長迫　智子

情報セキュリティ大学院大学
情報セキュリティ研究科
情報セキュリティ専攻

2023 年 3 月

(blank page)

Table of Contents

(blank page)

1. Preamble

“We live in the age of disinformation.”

This is according to security and intelligence researcher Thomas Rid[1].

Since time immemorial, 'information' and 'intelligence', the processed accumulation of such information, have been important decision-making factors for states in peacetime politics and in warfare. And, of course, for ordinary citizens as well, gathering 'intelligence' has remained important for individual decision-making, not only in political events such as the exercise of suffrage, but also in work and private life.

However, the development of the internet in recent years, and in particular the rise of social networking services, has changed the nature of information distribution. Information is no longer disseminated unilaterally by public authorities or the mass media, but can now be easily transmitted by the general public. This has led to a 'buzz' of 'information', sometimes containing major errors, and the instantaneous sharing of mixed information. This structure has led to a number of influence operations at the political level, where false or distorted information is deliberately mass-circulated in order to influence the politics of hostile countries, and at the civic level, where there is less resistance to posting false, deceptive or manipulated images to make oneself look good. The world has become increasingly disinformation-driven.

In these times, the security environment is also changing. This paper considers disinformation-based influence operations, of which the number of cases has increased in recent years in many countries, as a threat to security, conducts case studies and policy assessments from a security perspective, and makes policy recommendations based on these case studies and evaluations.

1-1. Background

The concept of the Internet was born with the standardisation of TCP/IP in 1982, and with the implementation of the World Wide Web in the 1990s, cyberspace constituted by the Internet has continued to expand dramatically. This cyberspace is now closely connected to real space through IoT devices, and furthermore, the development of social networking services (SNS) and web advertising on the Internet has connected even the cognitive space, such as the thoughts and feelings of ordinary citizens. With the expansion of cyberspace, the physical realm of reality, the virtual realm created by computers and the internet, and the cognitive realm of humans have come to merge and interact with each other.

With this growing influence of cyberspace, the threat of cyber-attacks has become humanity's greatest concern. Initially, cyber-attacks were mainly information-stealing cyber-attacks, in which criminals used cyber-technology to steal personal information and intellectual property information in order to make money. However, as malware evolved to facilitate function-destructive cyber-attacks, attacks on social systems and critical infrastructure began to take place. In addition, as it began to be

recognised that such attacks were effective as a form of state execution, state actors began to enter the fray as attack actors, not only for criminal groups with financial objectives, but also for information theft for intelligence purposes and for subversive activities as part of the use of force against other countries under armed attacks. And because cyberspace was easy to attack, interfere with and destabilise other states through information warfare, state actors attack actors began to attempt information-manipulating cyber-attacks. Against this background, influence operations centred on disinformation dissemination in cyberspace became more active, and cyberspace-based information warfare was waged in both peacetime and emergency situations. The battlefield now extends from land, sea, air and space to cyberspace and our own cognitive space, and not only soldiers in the armed forces but also all citizens are on the battlefield.

This is a major shift from the days when kinetic warfare was the predominant form of warfare, and we believe that it is an urgent global challenge to analyse the case and take appropriate countermeasures in the face of this new and growing security threat. Furthermore, information warfare, cognitive warfare and related events are themselves very abstract compared to traditional warfare events and are relatively new concepts, which means that definitions and terminology have not been organised and there is a lack of a shared awareness of the issues concerning the new threats.

Against this background, it was decided to take up cyberspace-based information warfare conducted by state actors, particularly disinformation-based influence operations, as a research topic.

The term Disinformation itself began to be used during the Cold War in the 1950s, mainly in the intelligence community around East and West Germany[2]. However, the range of influence operations by intelligence agencies was limited in both wartime and peacetime, and disinformation was a term used only between intelligence agencies.

However, with the advent of the internet, the situation changed. It became possible to spread information cheaply and instantly, and with the advent of social networking services, it became an interactive information network, and influence operations involving the general public on a large scale began to have an effect. In this context, contingency disinformation attracted attention during the 2014 Crimean conflict, peacetime disinformation attracted attention during the 2016 US presidential election, and cases of peacetime election interference accumulated thereafter.

In response to the Crimean conflict, the East StratCom Task Force was established in March 2015 as part of the EU's Action Plan on Strategic Communication to address disinformation campaigns waged by Russia, and In each country, countermeasure offices, task forces and other bodies have been established within government agencies, and legislative measures to combat disinformation have been developed. Against this background, surveys and research on disinformation have been conducted by government agencies in various countries. For this reason, this paper also refers to a number of government reports from various countries. In the field of research, there are journals centred on information warfare, such as Journal of Information Warfare[3], and research on the subject of

disinformation is also advancing in the fields of security and media studies. In addition, research that carries out computational analysis, such as diffusion factor analysis and cluster analysis of disinformation in SNS, is gaining momentum as a field of research related to disinformation, and in Japan, Professor Fujio Toriumi of the University of Tokyo and Kazutoshi Sasahara of Nagoya University are pioneering such research.

1-2. Objectives and Methods

The main focus of this paper is a case study of Disinformation and the formulation of a policy evaluation model based on it.

First, the paper defines the terms influence operations, disinformation and cognitive warfare, which have mixed meanings in relation to information warfare, in the context of this study with security as its scope. Then, using 2016, the year in which influence operations were reportedly carried out against the US presidential election, as a milestone year, the main cases of disinformation since then will be analysed, and the measures that countries have taken to counter the effects of disinformation will be discussed. The study also examined what measures countries have taken and what national strategies they are following. The measures taken focus in particular on the legal system, describing the limits of international legal countermeasures and providing an overview of the state of domestic legislation in each country. Based on these findings, an assessment model is developed to identify the national strategies that should be adopted in order to counter disinformation. Using this model, we will evaluate the policies of representative Western countries and Japan with regard to disinformation, and identify issues for Japan. The aim of this study is to make policy recommendations for Japan in accordance with the issues identified.

This study focuses on disinformation by foreign actors, and does not cover the dissemination of false information by the own citizens. This is because the regulation and countermeasures against the latter one are given more considerable weight in conflict with freedom of speech compared to the former one,[4] also considering the idea of self-determination, and this research targets disinformation as national security threat from the perspective of information warfare and cognitive warfare.

2. Overview of Information Warfare

In the current situation, these terms such as information warfare, influence operations, disinformation and cognitive warfare are used without precise definitions, causing confusion, which needs to be sorted out and discussed. There is an earlier argument saying that "lack of consensus when it comes to defining all the elements that make up the strategic application of power in the information domain"[5], but this discussion will attempt to sort out them.

In addition, as a result of people's mutual exchange of data and information in the cyberspace extended from the real physical space, particularly through social networking sites, information warfare and influence operations have been no longer the issue of information realm alone. As people's cognition is connected to the information network, the human cognitive domain is exposed to cyberattacks. Furthermore, only the question of correctness or incorrectness of information have already not considered, but also the strategy exploiting narratives to influence the international public opinion and the political regimes of hostile countries, which is known as the Battle of Narrative or Weaponized Narrative. Cyberspace is described to be the fifth battleground, but the human cognitive domain is now regarded as the sixth battleground.

Based on these issues, and after sorting out the current state of information warfare, this chapter discusses the definition of these factors in the context of national security.

2-1. The Definitions of Influence Operations

In this section, the definitions of NATO, US military and some other terms are referred to in order to organize the various operations around information warfare. The previous research of NATO describes that Influence operations are therefore an umbrella term covering all operations in the information domain, including all soft power activities.

It sorts Influence Operations as three sub operations; Inform & Influence Operations (IIOs), Influence Cyber Operations (ICOs) and Information Operations (IOs). These explains are quoted and complemented here.

> Influence Operations: The use of non-military (non-kinetic), means to erode the adversary's willpower, confuse and constrain his decision-making, and undermine his public support, so that victory can be attained without a shot being fired. They are also the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviours, or decisions by foreign target audiences that further (a nation's) interests and objectives'.
>
> Inform & Influence Operations (IIOs): Inform & Influence Operations are efforts to inform, influence, or persuade selected audiences through actions, utterances, signals, or messages.

Influence Cyber Operations (ICOs): Operations which affect the logical layer of cyberspace with the intention of influencing attitudes, behaviours, or decisions of target audiences.'

Information Operations (IOs): The integrated employment, during military operations, of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting its own.

This definition of IO relied on the US Depart of Defense definition[6], which defines it as a military capability. It involves various operations as following table.

IOs	Description
Psychological Operations (PSYOP)	Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.
Military Deception (MILDEC)	Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.
Operations Security (OPSEC)	A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identity those actions that can be observed by adversary intelligence systems; b. determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.
Electronic Warfare (EW)	Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support.

Computer Network Operations (CNO)	Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.

Table 1. US Military Information Operations Definitions (Joint Chiefs of Staff, 2010)

Additionally, other research[7] sorts of Influence Operations as 2 types of character which helps to understand features and directions of Influence Operations.

It describes that Influence Operations capabilities described above, four main objectives can be identified, which are: to influence/inform; to deceive; to deny/protect; and to exploit/attack. Following these lines, Influence Operations can be divided into two broad strands:

1. The first is technical influence operations (TIOs), which target the logical layers of the information space and include information delivery systems, data servers and network nodes. This strand thus includes operations such as EW, OPSEC, or OCO.
2. The second is social influence operations (SIOs) (aka. Information influence activities or cognitive influence activities), which are focused on the social and psychological aspects of information operations and aim to affect the will, behavior and morale of adversaries.

This research described that the strand includes elements out of the military playbook such as PSYOPS and MILDEC but also public affairs and military-civilian relations. SIOs can in turn be considered as a subset of influence operations but initially are limited to military operations in times of armed conflict at least for the US. Influence operations are, however at present, not limited to the military context, but form part of a larger effort by nations to exert power over adversaries in multiple spheres (i.e. military, diplomatic, economic). These efforts can, for example, involve targeted corruption; funding and setting up Potemkin villages (e.g. political parties, think thanks or academic institutions); putting in place coercive economic means; or exploiting ethnic, linguistic, regional, religious, and social tensions in society.

Based on the above discussion, here these terms around information warfare are visualized and applied to the latest case of Ukraine War in 2022 to assist to understand them, because the discussion concerning information warfare is more abstractive than that of the classical operational domains.

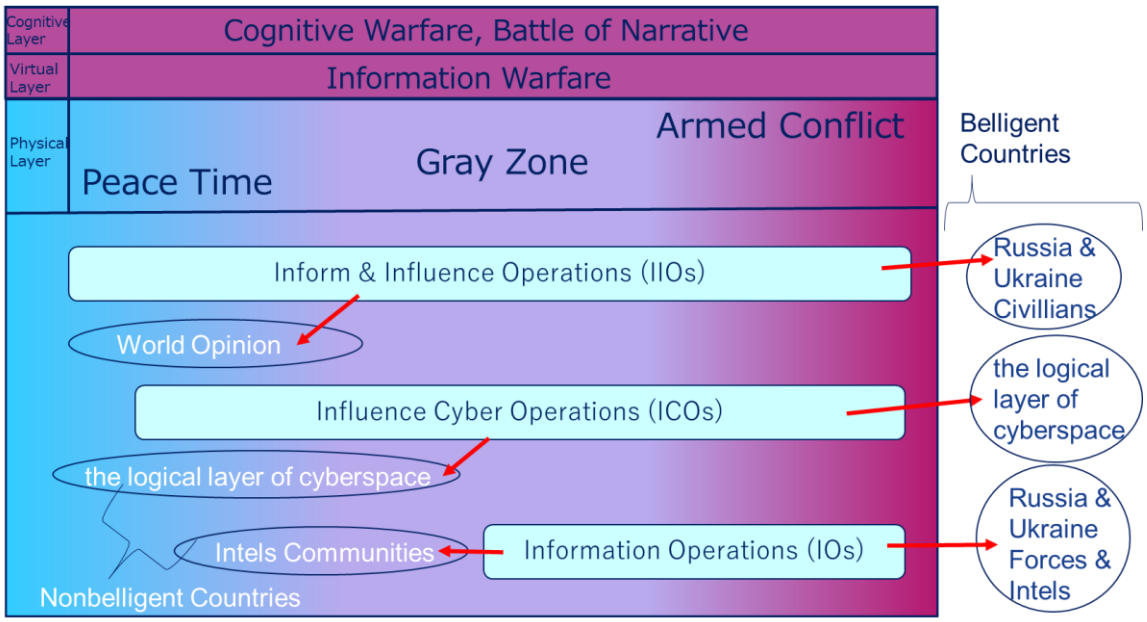

Fig. 1 Influence Operations Definitions by NATO applied to the case of Ukraine War (Based on "Influence Cyber Operations: The use of cyberattacks in support of Influence Operations," 2016, p117.)

In this war, there are three layers of information that Russia is attempting to influence; (i) narratives justifying Russia's invasion to international public opinion (=IIOs), (ii) disinformation with cyberattacks to confuse Ukrainian citizens and discredit the Ukraine government (=ICOs+IIOs), and (iii) military strategic deception operations (IOs). It is important to note that (ii) and (iii) also may play the role of narratives, and (i) may function not only to legitimise Russia but also to discredit Western societies, because they are syncretized with the national strategy in a complex process.

As for (i), these are the typical cases that narratives such as "the Ukrainian government is neo-Nazi and is committing genocide in pro-Russian areas in the east", "Ukraine and Russia are historically a unity", "NATO is threatening Russian security" have been disseminated since Euromaidan in 2013 and Crimean crisis in 2014, which were the abyss of the current military invasion. According to the website EUvsDisinfo[8], produced by the EU's East StratCom Task Force, 263 disinformation cases involving such narratives have been identified from January 2022, when Russian-Ukrainian tensions increased, to the end of April after the invasion. Meanwhile, 5,290 disinformation cases involving Ukraine have been identified since the establishment of the Task Force in 2015, which suggests that Russia has been conducting such influence operations continuously over a long period of time.

With these narratives as a background, Russian President Putin has claimed that the objective of the current military operation is mainly just to exercise the self-defence of Russia and protect the Donetsk and Luhansk People's Republics from the Ukrainian threat[9].

The next typical case of (ii) was the cyber-attack on the Ministry of Defence of Ukraine and two national banks (Oschad and Privat) on 15 February, and the disinformation disseminated in relation to them. Initially, the distributed denial of service (DDoS) attacks on the websites of these two banks caused the websites to go down. The US and UK authorities have determined that this cyber-attack was carried out by the Russian GRU[10]. Around that time, disinformation was sent to Ukrainian citizens via SMS (short message service), spoofing these banks and claiming that their ATMs had become inoperable. This disinformation spread confusion among citizens for a time, but the citizens themselves confirmed that the ATMs were in fact functioning and refuted the malicious attackers on social networking sites. The attacks had two objectives, according to US security giant Mandiant[11]: the first was driving consumers to the bank websites, contributing to the ongoing DDoS attacks, and the second, and perhaps more important, was “driving up that fear, driving up the uncertainty around, ‘Can the Ukrainian government protect itself?”.

As for (iii), the announcement by the Russian Defence Ministry[12], also on 15 February, that Russian military units had finished their exercises and started withdrawing, is probably the best example. This was deceptive information to blitz the "special military operation” but was refuted by the Western media through analysis of commercial satellite images, images and videos posted on SNS and so on. Furthermore, the operation failed, as on 18 February, US President Joe Biden denied this announcement in his remarks[13], saying that he was convinced, based on US intelligence information, that Russian President Vladimir Putin had decided to invade Ukraine.

In the discussion surrounding such information warfare, it can be said that disinformation and narratives are tools of Influence Operations and that it is mainly used in peacetime and in the grey zone. This is because, as previous studies[14] have shown, disinformation targets the political system and democratic processes of the opponent, increasing social contradictions and tensions and distorting the decision-making of the opposing nations.

Additionally, narratives strategically created by the state stimulate and invade the cognitive domains of memory, experience, values, reasoning and emotions of all those who are exposed to information regarding the narrative, and they are ultimately completed in the cognitive domain of the individual. In the above example, with regard to the narrative justifying the Russian invasion, the extent to which an individual reflexively accepts or rejects it depends on the functioning of his or her cognition, when exposed to this narrative before confirming it is fact or not. In other words, the field of information warfare has extended into our cognitive domain, hence the term 'cognitive warfare'. These points are discussed in more detail in the subsequent sections.

2-2. The Definition of Disinformation

Since Russia's election meddling in the 2016 US presidential election attracted attention, similar operations by Russia or China are unveiled year by year. As the cases have reported increasingly, the term of disinformation seems to be heard more often. 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. The word of *fake news* describes just false news or false information, and it cannot figure out the whole image of this threat, because disinformation is a part of the influence operation, based on the national strategies and the complicated geopolitical purposes.

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

The European Commission's report[15] 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. 2) 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 European Commission[16] also defined *disinformation* as all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit.

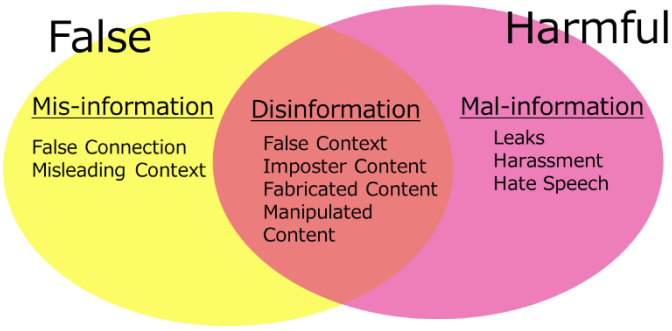

Fig. 2 Definition **of Disinformation by EU**

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

For example, in the US presidential election of 2016, the Office of the Director of National Intelligence's report[17] 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 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 contains the possibility of truth. In this election period, hate speeches that clamed Macron was gay. This harassment was spread widely on some media and SNS[18]. Indeed, in this case, these were fake news because Macron denied being gay[19] but, if these are true, are these hate speeches not as effective as disinformation? It is not 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 to make a social divide wider and damage democracy. The state actors distort and manipulate the contents of hate speech. So, disinformation that is operated in the frame of the national strategy should be distinguished from ordinary hate speech, and even if it's correct, harmful information should be guarded against.

Fig. 3 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 the multiple perspectives of disinformation are not completely understood, it would be difficult to find appropriate measures for this sophisticated information warfare.

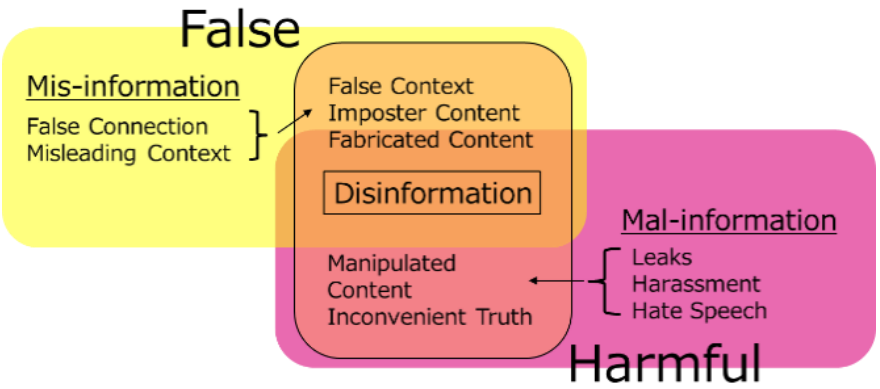

Fig. 3 Modified Definition of Disinformation by the author

Furthermore, as the issue of disinformation clashing with freedom of expression is mainly an internal affair of a country[20], the security study regarding disinformation from the perspective of national security and strategy should focus on the operation conducted by foreign actors. This approach is followed in this study, and the case of Japan is discussed in the chapter 7-2.

2-3. The Definition of Cognitive Warfare

This section starts with another challenging term "narrative" in the context of national security, which is mentioned in the above section initially.

Narrative is, according to the definition by Marc Laity who was a chief of strategic communications at SHAPE (Supreme Headquarters Allied Powers Europe), NATO's military headquarters in charge of alliance military operations when he wrote the paper[21], "more than just a story. Rather, a narrative contains many stories, and—more importantly—it is an explanation of events in line with an ideology, theory, or belief, and one that points the way to future actions. Narratives make sense of the world, put things in their place according to our experience, and then tell us what to do. A strategic narrative aligns the strategy and the narrative, so they become mutually supportive and integrated."

So as to understand the mode in which strategies are transformed and exercised in narratives, the following specific comparisons by Laity[22] will help to understand this.

In Ukraine the Kremlin's strategy could be described thus:

In order to put pressure on, and regain influence over, the Kiev government and prevent its westward orientation, we will use covert action and, if necessary, further military means to increase and exploit pro-Russian sympathies, regain Crimea, and support a pro-Russian enclave in Ukraine.

However, expressed in Russian media narratives, this can sound like:

The fascist junta in Kiev illegally toppled the elected government and is viciously oppressing our Russian compatriots in Ukraine, who desperately needed and called for our help to protect their culture and rights.

Essentially these two statements are saying the same thing, even if the first couches it in operational-style language and the second in emotional terms. In effect, this is a strategy expressed in narrative form.

This strategic exercise of narratives by the state is the battle of narratives. Narratives are mainly constructed from disinformation. They may contain facts, but as identified in the previous section, they are distorted in context or conceal inconvenient truths which are strategically and maliciously manipulated. This is similar to the flow of a great river. The river of narratives is strategically

contaminated by the mixture of pollutants called disinformation, but it is very difficult to compartmentalise and eliminate them in the stream of information.

As discussed above, under the battle of narrative, the influence operations exploiting narratives target the line with an ideology, theory, or belief, and one that points the way to future actions. This line is generated from the human cognitive information processing[23]. (See Fig. ★) As such, the battlefield is now perceived as extending into our cognitive domain. This is known as cognitive warfare.

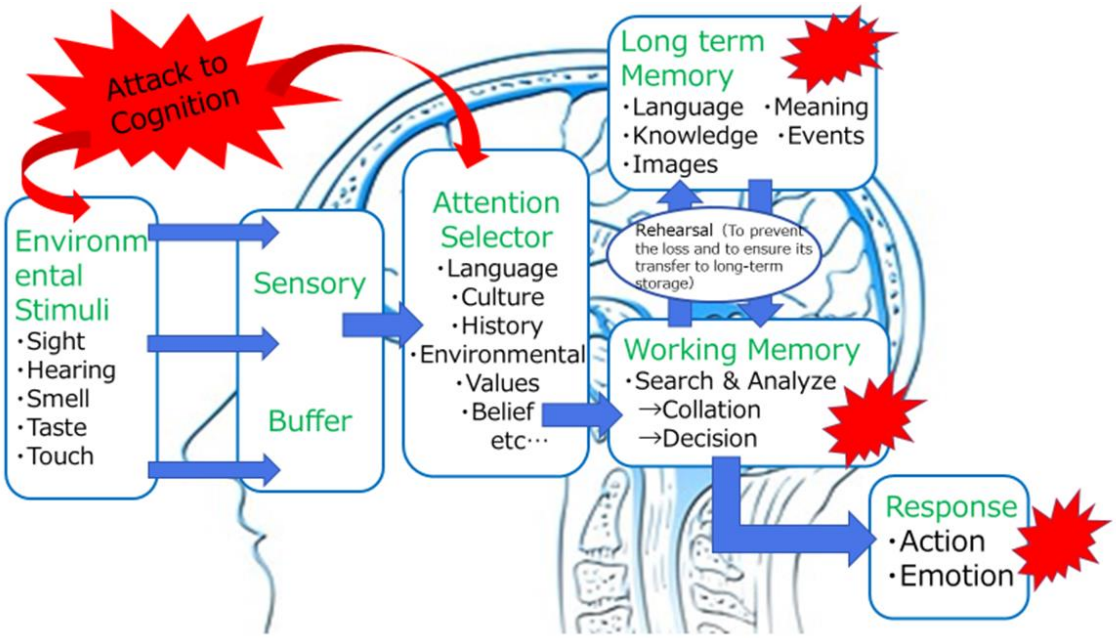

Fig. 4 The processing of the attacks to human cognition.

(Translated from SPF, 2022, "Prepare for Foreign Disinformation! -Threat of Information Manipulation in Cyberspace-" https://www.spf.org/security/publications/20220207_cyber.html)

In 2017, US Defense Intelligence Agency[24] or Air Force[25] started to mention the concept "cognitive warfare". Additionally, NATO Innovation Hub launched Cognitive Warfare Project in 2020[26]. As a result of these developments, a number of countries have started to work on cognitive warfare, but in practice, no established definition of cognitive warfare has yet been formulated. However, these definitions have the similar core idea of weaponizing the cognition of everyone and destabilizing the order and the establishment.

NATO's research[27] describes "cognitive warfare pursues the objective of undermining trust (public trust in electoral processes, trust in institutions, allies, politicians…)., therefore the individual becomes the weapon, while the goal is not to attack what individuals think but rather the way they think. It has the potential to unravel the entire social contract that underpins societies". Other definitions are ""an

amplified version of psychological warfare with the goals of dividing an enemy nation's people and leadership along social, economic, and political lines, destroying them from the inside without firing a shot" by Alderman[28], "manipulation of the public discourse by external elements seeking to undermine social unity or damage public trust in the political system" by Rosner and Siman-Tov[29], and "it is a disinformation process to psychologically wear down the receivers of the information" by Mackiewicz[30].

On the other hand, Captain Paul Ottewell[31], who is a Royal Navy warfare officer, criticises these definitions as having a somewhat negative bias and offers the following more neutral definition; cognitive warfare is manoeuvres in the cognitive domain to establish a predetermined perception among a target audience in order to gain advantage over another party, after he defined cognitive domain as "a domain consisting of perception and reasoning in which manoeuvre is achieved by exploiting the information environment to influence interconnected beliefs, values, and culture of individuals, groups, and/or populations".

Ultimately, cognitive warfare focuses on gaining an advantage over the opposing state and remaking it into a social and political system favourable to one's own country. Additionally, it should be aware of the threat that the cognitive domain is being weaponised in war, thereby putting all citizens, not just soldiers, on the battlefield of cognitive warfare.

However, the question arises whether cognitive warfare, a completely non-kinetic approach, can be considered warfare in the first place. In this point, the discussion by Bjørgul[32] is instructive. To approach this question, the discussion starts with the U.N. Charter, which defines the limits of warfare. Article 2(4) prohibits the "threat or use of force against the territorial integrity or political independence of any state." The main exception from the prohibition of use of force is expressed in Article 51, which allows for "self-defense if an armed attack occurs against a Member of the United Nations." In this approach, it refers to the argument of whether a cyberattack constitutes the use of force, and from the idea that whether significant physical effects occur affects the threshold for the use of force, operations in the cognitive domain are concluded not to be applied to this framework.

At the same time, this argument also returns to the most classical definition of war by Clausewitz; "war is an act of violence in order to force our will upon the enemy[33]," because Ottewell's definition conforms to it. Here, this argument can be extended also to the aim of war. Clausewitz classified the objectives of war into two broad categories, war to achieve limited aims and war to "disarm" the enemy: to render him politically helpless or militarily impotent. The description on the latter is quoted below.

"If our opponent is to be made to comply with our will, we must place him in a situation which is more oppressive to him than the sacrifice which we demand; but the disadvantages of this position must naturally not be of a transitory nature, at least in appearance, otherwise the enemy, instead of

yielding, will hold out, in the prospect of a change for the better. Every change in this position which is produced by a continuation of the war, should therefore be a change for the worse, at least, in idea. The worst position in which a belligerent can be placed is that of being completely disarmed. If, therefore, the enemy is to be reduced to submission by an act of war, he must either be positively disarmed or placed in such a position that he is threatened with it according to probability. From this it follows that the disarming or overthrow of the enemy, whichever we call it, must always be the aim of warfare."

This aim, especially in this part "at least, in idea", is very applicable to the operations in cognitive domain. Distorting an opponent's political system to one's own advantage through influence operations such as election interference from peacetime, is precisely this war of disarming. From these arguments, operations by state actors in the cognitive domain can be conceptually described as cognitive warfare. On the other hand, although not on the threshold of use of force, the UN Charter was formulated at a time when kinetic means were predominant, and the definition of war may need to be revised. Under the new trend of democratic institutions and values being articulated as concrete property in the form of infrastructure, such as the designation of elections as critical infrastructure in the US, the debate on international law may also need to take a novel turn.

Finally, it is also important to point out that cognitive warfare is spreading due to its association with conspiracy theories, because physical destruction is occurring in the real world as a result of this nexus.

Recent report[34] suggests that several countries, including Russia and China, have 'weaponised' QAnon conspiracy theories to cause social discord and endanger legitimate political processes. It has also been named by the ODNI[35] and [36]FBI as a terrorist threat group since 2019. As for typical cases of conspiracy incident might lead the physical attacks, in January 2021, a QAnon gang attacked the US Capitol, and in 2022 a group of Reichsbürger members influenced ideologically by QAnon were arrested in Germany for attempting a coup d'état. In this incident in Germany, authorities have suggested also Russian involvement[37].

One of research[38] points out that the diffusion mechanism of conspiracy theories exploits existing oppositional structures, which is similar to the diffusion structure of disinformation noted in the previous section. Those who are deeply committed to one of the two camps of argument tend to jump on an opinion if it is favourable to them, regardless of whether it is true or not.

In more detail, another analysis[39] shows that cognitive traits such as conjunction fallacy, need for cognitive closure, cheater detectors, intentionally bias, crippled epistemologies and motivated reasoning influence the structure of conspiracy beliefs. Moreover, these characteristics indicate that clusters of conspiracy theorists can easily expand, and it is noted that the cluster that spread pro-Russian posts in Japanese on the invasion of Ukraine in Twitter had already disseminated content

sympathetic to QAnon and conspiracy theory regarding the vaccine for Covid 19[40].

In other words, cognitive traits of conspiracy theorists make it easy to control and weaponise them, and cognitive warfare targeting human cognition is very compatible with conspiracy theories. It will be necessary to take multifaceted measures to address this new development in cognitive warfare as a security threat.

3. Case Study of Disinformation

3-1. World Trends

This section shows the trends of disinformation in this world.

As a part of disinformation, the first focus is on election meddling. According to the report[41] 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%)[42]. 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)[43]. 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[44]. 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.

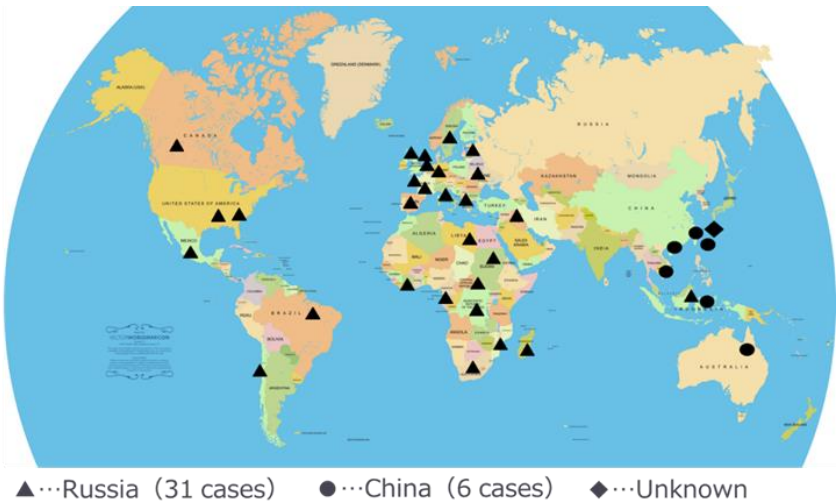

Fig. 5 Disinformation Cases (since 2016)

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

	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	Unknown
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

2020

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

Table 2 Disinformation cases (since 2016-2020)

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.

And then, since 2020, the trend has changed by Covid-19 and Ukraine War. Around covid19, China and Russia actively exploited disinformation that would improve their own reputations and conspiracy theories related to the origins of the virus and vaccination. Similarly, from late 2021 onwards, when tensions between Russia and Ukraine increased, narratives were actively disseminated which, as discussed in chapter 2 and below, portrayed Ukraine as a Nazi and NATO as a threat to Russian security. In parallel, influence operations aimed at election meddling continued, but the year 2020 is considered

a break for the case study analysis, as it is difficult to relate to and assess this trend change at the present. Future work is needed on the changing trend and continued case analysis.

3-2. Cases in Peacetime

In this section, details of major cases of influence operation exploiting disinformation are described to assist to understand the actual phenomenon of such operations.

3-2-1. US

In May 2016, the US Democratic National Committee was cyber-attacked and more than 19,000 emails of committee officials were stolen by hackers. These emails were published on whistleblowing websites WikiLeaks and DC Leaks.com, exposing that Democratic National Committee officials had deliberately worked to unseat Senator Bernie Sanders, who was competing with former Secretary of State Hillary Clinton for the presidential nomination. The leak was made public by the National Committee of the Democratic Party (NCP). The leaks led to the resignation of the Democratic National Committee chairman the day before the national convention, discrediting the Democratic executive. The quantitative impact of this attack on the outcome of the presidential vote has not yet been revealed, but the result was that the primaries were overturned and President Donald Trump was elected. A report[45] by the National Cybersecurity and Communications Integration Centre (NCCIC) under the Department of Homeland Security (DHS) published in December 2016, shortly after the election, identified two different types of cyber-attacks: 'Fancy Bear' (also known as 'APT28') involving the General Directorate of Intelligence of the General Staff of the Armed Forces of the Russian Federation (GRU) and 'Cozy Bear' (also known as 'Office Monkeys', 'Cozy Car', 'Cozy Duke' and 'APT29') involved in the attacks.

At the same time, there have also been reports of cyber-attacks involving Russia in the form of the dissemination of fake news and disinformation in favour of Trump and against Clinton's reputation on social networking sites, including Twitter and Facebook, during this election. An investigation[46] by the US House and Senate Intelligence Committees found that 2,752 Twitter and 470 Facebook accounts, approximately 120 Facebook pages and more than 80,000 associated page content were used by the Russian Government to conduct operations. The company also admitted to spending the equivalent of USD 100,000 to purchase 3,393 Facebook advertising spaces for Russian government agencies.

The Internet Research Agency (IRA), which was located in St Petersburg, organised the writing of such false or pro-Trump biased information using a 'troll unit' to manipulate online public opinion. Although superficially disguised as a private company funded by a nascent conglomerate, the conglomerate has close ties to the GRU and to President Vladimir Putin, as noted in a report[47] by the Office of the Director of National Intelligence (ODNI) of the United States. It also assessed that these

IRA activities were not voluntary patriotic activities by a private company, but state-sponsored operations, stating.

> "We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the USpresidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments[48]."

During the 2018 midterm elections, it was also revealed that cyber-attacks were carried out against the National Republican Congressional Committee (NRCC), with emails of the committee's leadership being stolen for several months[49]. However, unlike the 2016 attack on the US Democratic National Committee, it has not been confirmed that the emails were misused. In addition to this, cyber-attacks and influence operations have been reported by US intelligence agencies from Russia, China and Iran[50].

To counter these foreign powers, the US has adopted a Defence Forward (DF) strategy to counter cyber-attacks. The US Cyber Command (USCYBERCOM) blocked internet access by the Russian IRA for several days from 6 November 2018, the day of the midterm elections. It also identified Russian agents engaged in such election interference and displayed on-screen warning messages such as 'We are monitoring your operations' and 'You are subject to prosecution and sanctions'[51]. This was the first instance of the US military taking defensive action against election interference by a foreign actor.

During the US presidential election in November 2020, US intelligence agencies also assessed that Russia and Iran conducted cyber-attacks and disinformation activities with the aim of influencing the election[52]. As for China, the assessment is that it considered influence operations but did not actually carry them out, but cyber-attacks by China on election officials were confirmed before the election, and there is a minority opinion within the intelligence community that there were intentions and various activities to try to influence the election. The election was also characterised by the use of Q Anon, a movement in the US that espouses conspiracy theories. The fact that Q Anon and members of the Trump-supporting far-right movement went so far as to storm the US Capitol after the election is a clear example of how effective Russian disinformation can be in exploiting social contradictions and divisions.

3-2-2. UK

The referendum on 23 June 2016 in the UK to leave the EU has been implicated by Russia. The result of the vote was 16,141,241 votes in favour of remaining in the EU (approximately 48%) and 17,410,742 votes in favour of leaving the EU (approximately 52%), with the pro-leave side winning

by a narrow margin.

However, as in the US presidential election, an interim report by the UK House of Commons' Culture[53], Media and Sport Committee revealed that the Russian IRA was involved in shaping public opinion in favour of Leave. An investigation of some 2,700 Twitter accounts and 4,000 Facebook accounts implicated by the IRA in the US presidential election confirmed that these accounts repeatedly posted in support of and inducements to leave the EU in the UK referendum as well. There are also suspicions that accounts that did not interfere in the US presidential election also interfered in the UK referendum with the involvement of the IRA, leading the Commission's chair Damian Collins to request that the CEOs of Twitter and Facebook provide a list of accounts with links to Russia[54].

At this stage, investigations have not identified any direct cyber-attacks on the referendum, and it is believed that the interference was mainly through the disinformation disseminated by social networking sites.

3-2-3. Germany

In the German Bundestag elections (general election) held on 24 September 2017, out of a total of 709 seats, Merkel's ruling party, the German Christian Democratic Union/Christian Social Union Unity Party (CDU/CSU), won 246 seats (311 seats previously) to become the leading party and Merkel will continue in office for a fourth term Merkel will continue for a fourth term. The centre-left Social Democrats (SPD) followed with 153 seats (previously 192) to become the second largest party. However, the CDU/CSU's share of the vote was the lowest since 1949 and the SPD's share of the vote the lowest since 1933, and both parties accordingly saw their seats reduced significantly from the previous round. On the other hand, the emerging right-wing party Alternative for Germany (AfD), which advocates leaving the EU and opposes refugees, made a significant leap forward, winning 94 seats, securing a seat in the Bundestag for the first time and positioning itself as the third party.

In Germany, as in the UK, there were no direct cyber-attacks in this election, as in the 2016 US presidential election, but mainly interference by Russian-related media and disinformation spread by the IRA on social networking sites. Characteristic in Germany was the use of bot accounts and the dissemination of fake news by Russian-affiliated media. These developments were seen even before the elections, a typical example being the 'Lisa case' reported in January 2016[55]. The incident, in which a 13-year-old Russian-German girl was raped by a group of refugee Arab men, was repeatedly and persistently reported through Russian government-owned media channels 1, RT and Sputnik, and spread through relevant social networking accounts. In fact, although the incident was untrue, the Russian-affiliated media and personal accounts that fuelled it actually led to a number of demonstrations and rallies across the country criticising the incident and advocating anti-refugee policies.

Also in March 2016, a photo purported to be a selfie with Chancellor Merkel by the perpetrators of

a series of bombings in Belgium was spread, along with the perpetrators' mug shots. In reality, the former was a photograph taken by Chancellor Merkel with a young Syrian refugee during a visit to a refugee centre in Berlin. When the youth uploaded the photo to his Facebook page, which was doctored with the wrong caption and uploaded to the Anonymous-affiliated page 'Anonymous Collective' on the Russian-affiliated social media site Hukontakte, it was spread on social networks starting with the article and became the article became fodder for criticism of Merkel's immigration policy and the spread of pro-AfD discourse[56].

It has been confirmed that during the election period, there were approximately 350,000 posts in support of the AfD on Facebook and more than 2.5 times the amount on Twitter compared to other parties[57]. The considerable volume compared to the vote share suggests that a significant number of bot accounts associated with Russia were in operation[58]. A trend of support for AfD policies was thus deliberately created.

Prior to the Bundestag elections held on 26 September 2021, there were hacking attacks against the CDU and Parliament earlier that year. In addition, at the end of August, the website of the Federal Decretariat, the organisation responsible for publishing the official results of the upcoming parliamentary elections, was temporarily unavailable due to DDoS attacks that sent large amounts of data[59]. In addition, by September, phishing attacks had been confirmed, in which information was stolen by directing users to disinformation websites for parliamentarians, political party officials and others[60]. On 6 September, just before the elections, the German Government condemned cyber-attacks of data theft that could be preparations for information warfare in connection with the Bundestag elections. The German Government stated that it had "reliable information" that allowed it to determine that these activities were "by Russian state actors, in particular by the Russian military intelligence agency GRU" and called on Russia to cease these cyber-attacks[61]. The Bundestag Election Commission also publishes[62] the main disinformation disseminated during the election period, along with corrected information, which also confirms that some of the discourses, including those on postal vote rigging, were spread by the AfD[63].

3-2-4. France

There was also electoral interference in the French presidential election in May 2017, and the methods used were of the same type as in the 2016 US election.

First, it was reported that cyber-attacks were carried out on the Electoral Commission and the Secretariat of the Republican Forward Party led by Macron about six months before the election, and that some data was actually stolen through phishing emails and other means.

This was carried out by the same group that hacked the Democratic National Committee in the US, APT28[64]. However, unlike in the US, no clear information on the scandal was available, and the Russians also created and disseminated fake news. In programmes and articles by Russian

government-affiliated media outlet RT and Sputnik's French bureau, opinions such as "a pawn of the US industrial finance industry", "gay" and "defender of Islam" were repeatedly transmitted in reference to Macron, which were then spread on social networking sites. At the same time, opinions in support of the National Front, which foments the crisis caused by Muslim immigration and opposes it, were also massively disseminated via bot accounts[65].

As a result, Emmanuel Macron (Republic Forward) won 66% of the vote in the French presidential election run-off on 7 May (24% in the first round of voting), ahead of Marine Le Pen (National Front. He defeated Marine Le Pen (National Front) with 33% of the vote [21% in the first round of voting]) to become President.

However, the election results of the first round of voting, held on 23 April before the run-off, were unparalleled. This was because for the first time in the history of the Fifth Republic, neither the right-wing Republican Party nor the left-wing Socialist Party was able to field a candidate in the run-off vote. It was also the first time in history that the National Front kept its candidate until the deciding vote. Because of its anti-EU and anti-immigration platform, the National Front is close politically to Russia and indeed receives financial support from the Russian government. Russian election interference in France involved attacking Macron and supporting Le Pen and other right-wing candidates.

3-2-5. EU

With regard to the 2019 European Parliament elections, the Commission's report[66] assesses that it has "identified ongoing disinformation activities by Russia aimed at reducing voter turnout and changing voting behaviour" affecting voters in the European Parliament elections. The Commission's investigation found that around 1,000 cases of disinformation on websites aimed at spreading extremist views and polarising public opinion on issues of immigration and religion were identified, doubling compared to the same period the previous year. The methods used included the use of social networking accounts and the creation of fake news websites to disseminate disinformation. The European Commission has criticised these developments as activities that undermine EU values and has called on platform operators of social networking sites such as Facebook and Twitter to further strengthen their measures.

3-2-6. Taiwan

In Taiwan, there have been indications of manipulative attacks on public opinion from China in the presidential and local elections.

In the 16 January 2016 presidential election, President Tsai Ing-wen of the DPP, who has distanced herself from China, won 56% of the vote (31% for KMT President Chu Li-lun and 13% for pro-PMT President Song Chu-yuen), and there appeared to be no Chinese influence. However, prior to the

election, 'spear-phishing' attacks were carried out against Taiwanese government officials and Taiwan independence campaigners, sending disinformation to specific organisations and individuals through disinformation emails, and it has been pointed out that the hacker group APT12, which is analysed as having strong links to the Chinese People's Liberation Army, was involved in these attacks[67]. No disinformation dissemination or any kind of manipulation of public opinion using leaked information from these attacks was observed. There were also 50,000 acts of 'trolling' in the Facebook comments section of elected President Tsai in the immediate aftermath of this election[68].

In the 2018 local elections, the DPP suffered a heavy defeat and "recently, there has been a flow of untrue and false information from China, all of which are pressure measures intended to intervene in Taiwan's democratic elections. These situations have been witnessed by all circles together and are already universally recognised facts by the international community", commented a DPP spokesperson[69], but the specifics of the attacks were not made clear. The DPP's interpretation[70] of the DPP candidate's defeat in the Kaohsiung mayoral election is that Chinese patriotic netizens pulled Taiwanese public opinion with their numbers, as the video posted on the video-sharing website You Tube by his opponent, KMT's Han Guo-yu, received over a million "high ratings". It appears that disinformation techniques of mass dissemination of positive opinions of specific candidates, rather than explicit attacks, were used.

In the 11 January 2020 presidential election, incumbent President Tsai of the ruling Democratic Progressive Party (DPP) won a landslide victory with approximately 8.2 million votes (57% of the vote). Her opponent, Han, the candidate of the largest opposition party, the Kuomintang (KMT), who argued that stronger relations with China would bring economic benefits to Taiwan, received approximately 5.5 million votes (39% of the vote). During this election period, President Tsai expressed her alarm at the election intervention, saying that "China has fully 'infiltrated' [Taiwanese society]", while Han, the opposition candidate, criticised President Tsai for using the election to stir up anti-Chinese sentiment, and the two candidates disagreed on China's intervention[71].

Post-election analyses by Taiwanese authorities and US think tanks suggest that there was also Chinese intervention in the same election[72]. According to an analysis by the US think tank Center for Strategic and International Studies (CSIS), the Chinese Communist Party (CCP) has encouraged Taiwanese nationals and their families residing in mainland China to return home and vote for pro-China candidates, infiltrated the Taiwanese press, and conducted pro-China reporting and self-censorship in order to increase support for pro-China candidates and manipulate public opinion. CSIS assesses that as a result, support for the Chinese government's preferred candidate has increased[73]. In addition, according to reports in Taiwan, the Taiwanese Government is investigating more than 30 cases of alleged CCP funding of the election campaigns of candidates running against the DPP.

The CCP is alleged to have (i) provided funds to Taiwanese media organisations and polling companies to produce and publish fake survey results that favour pro-China candidates, (ii) organised

the "Five-Headed Party", which receives rewards for posting comments, to attack anti-China candidates on Facebook and other social networking sites and make them post pro-China comments, among other activities. The "Five-Headed Party" is said to be engaged in such activities. In fact, the number of attacks by the "Five-Headed Party" on Taiwanese websites per day has reached at least 2,500.

3-2-7. Hong Kong

In Hong Kong, the Chinese government is conducting a manipulative public opinion attack on the democratic process of demonstrations rather than specific elections: in March 2019, the Fugitive Offenders Ordinance amendment triggered democracy demonstrations in Hong Kong, aiming for the complete withdrawal of the Fugitive Offenders Ordinance amendment and the realisation of universal suffrage. In response, the Chinese Government is alleged to have attempted to manipulate public opinion by using state media articles and distributed advertisements on Twitter and Facebook to create the impression that these demonstrations were unjustified and instigated by terrorists influenced by western countries and extremists[74].

In connection with this information operation, 963 accounts were identified on Twitter and over 200,000 spam networks were suspended; on Facebook, five accounts, seven pages followed by over 15,000 accounts and three followed by around 2,200 accounts groups were suspended. In both announcements, it was assessed, based on evidence, that these were activities supported by the Chinese Government and were deliberate attempts to cause political discord in Hong Kong[75].

3-2-8. Japan

In Japan, unlike in other countries, no clear cases of foreign disinformation have been identified. The reasons for this are the peculiarities of the Japanese language space and the existence of Japan's own SNS platforms. However, there have been scattered cases of security concerns.

On 3 October 2019, the Ryukyu Shimpo reported on its front page that the US was planning to deploy a new medium-range ballistic missile in Okinawa and had already informed the Russian side[76]. This report was information provided to the Ryukyu Shimpo by a Russian government official. On 18 October, during Okinawa Governor Denny Tamaki's visit to the US, he confirmed the report with Pentagon officials, who denied that there was any such deployment plan. With regard to the reports, it has been suggested that they were deliberately circulated by the Russian Government, which is concerned about the destruction of the Intermediate-Range Nuclear Forces (INF).

Another case in point is the 2018 Okinawa gubernatorial election. Although not explicitly identified as disinformation from a foreign power, the type of disinformation and the security significance of the point of origin should be kept under close watch and consideration.

During the 2018 Okinawa gubernatorial election, websites called 'Okinawa Prefectural Governor

Election 2018' and 'OkinawaBaseIssues.com' were created, and the 'fake news' posted by these websites that undermined then candidate Tamaki, an opponent of the US military base construction, and the late former governor Onaga Takeshi, also an opponent, was spread through social networking services. The Ryukyu Shimpo and Okinawa Times conducted fact-checks on the content of the messages and confirmed that they were 'fake news'[77]. However, the source of the information was investigated by the Ryukyu Shimpo, but was never clarified[78].

It is said that the fake news disseminated was likely to have originated from opposition forces in Japan, as it was false information about Tamaki's campaign and showed an anti-Tamaki stance. However, disinformation can also be made with the aim of undermining the credibility and legitimacy of elections in a democracy by planting doubt in the results or giving the impression that the results are not legitimate. Therefore, it is necessary to consider the possibility that this case is not simply part of an unsuccessful election campaign, but also an attack by forces aiming to damage democracy.

From this perspective, the possibility of interference by foreign powers cannot be completely ruled out, such as China[79], which is reportedly trying to shape public opinion in Okinawa through the undecided theory of belonging to the Ryukyu Islands, and Russia[80], which has stated that the US military bases in Okinawa are an obstacle to Japan-Russia relations and has been trying to get closer to Okinawa in recent years[81].

3-3. Case in Wartime

This section reviews disinformation cases in Ukraine war involving the cases before the war happened.

In January 2022, the US State Department published examples of Russian disinformation and fact-check results in the Russia-Ukraine crisis[82]. In this fact sheet, following disinformation discourses were objected.

・Ukraine and Ukrainian government officials are the aggressor in the Russia-Ukraine relationship.
・The West is pushing Ukraine toward a conflict.
・Russia’s deployment of combat forces is a mere repositioning of troops on its own territory.
・The United States has planned chemical weapons attacks in the Donbas.
・Russia is defending ethnic Russians in Ukraine.
・NATO has plotted against Russia since the end of the Cold War, encircled Russia with forces, broken supposed promises not to enlarge, and threatened Russia’s security with the prospect of Ukrainian membership in the Alliance .
・The West shuns diplomacy and goes straight to measures like sanctions.

In addition, cases of disinformation captured by NATO are also examined[83]. Since the beginning of the year, when the Ukrainian crisis escalated, there were 225 Ukraine-related disinformation cases identified by the NATO/Hybrid Threat Centre in the period 1/1/2022 - 15/4/2022. Broadly, these include: 'Ukraine is a neo-Nazi power'; 'Ukrainian forces are massacring pro-Russian groups in eastern Ukraine'; 'Ukrainian forces are using chemical and biological weapons in violation of international law'; and 'Russia's original origin is in Kiev'.

These can be seen as justifications for Russia's invasion, discrediting Ukraine, dividing Ukraine and the West, and appealing to the unity of Russia and Ukraine. Here, disinformation and narratives are intricately intertwined.

On the one hand, when fake news was released from Russia that President Zelensky, who is also conducting information warfare as a counter to Ukraine, had fled Kiev, President Zelensky stayed in Kiev and actively sent out videos on social networks to fight against the war. Ukrainian citizens also cooperated, uploading videos on social networking sites showing attacks on the city and testimonies of captured Russian soldiers who were brought in under the guise of exercises, to appeal to international public opinion. It is not simply that Ukraine is countering with correct information, but the Ukrainian side is also utilising fakes. By reporting that captured Ukrainian border guards were crushed, and by misinforming the public that there was an increase in radiation levels during the attack on the Chernobyl nuclear power plant, it can be said that Russia is the bad guy and Ukraine is the poor victim.

In addition, on 15 February 2022, just before the military invasion, the media simultaneously reported that Russian troops had begun withdrawing, and President Putin indicated that he would continue consultations with the West[84]. However, the US side disclosed a certain degree of intelligence and denied the move in a speech by US President Biden on 18 February[85]. President Biden said that "Russia has increased its forces along the border by about 7,000", "I am convinced that at this point he [President Putin] has made the decision [to invade Ukraine]" and "I have reason to believe that Russian forces have plans, intentions, to attack Ukraine next week, that is, within a few days. The targets will include the Ukrainian capital of Kiev", he stated. This is not disinformation, but rather an Information Operation with a primary focus on military influence.

4. National Strategies of State Actors

This chapter reviews what regimes and strategies Russia and China employ to wage information warfare.

4-1. Intelligence Capability

4-1-1. Russia

The main government agencies involved in cybersecurity in Russia are shown in the figure below, but the division of roles among the relevant agencies for ensuring cybersecurity is not clear and there is currently no single coordinating agency to facilitate inter-ministerial cooperation and other activities. Therefore, there are often jurisdictional disputes over cyber-related matters, such as the competing hacking activities of different Russian government agencies during the 2016 US presidential election.

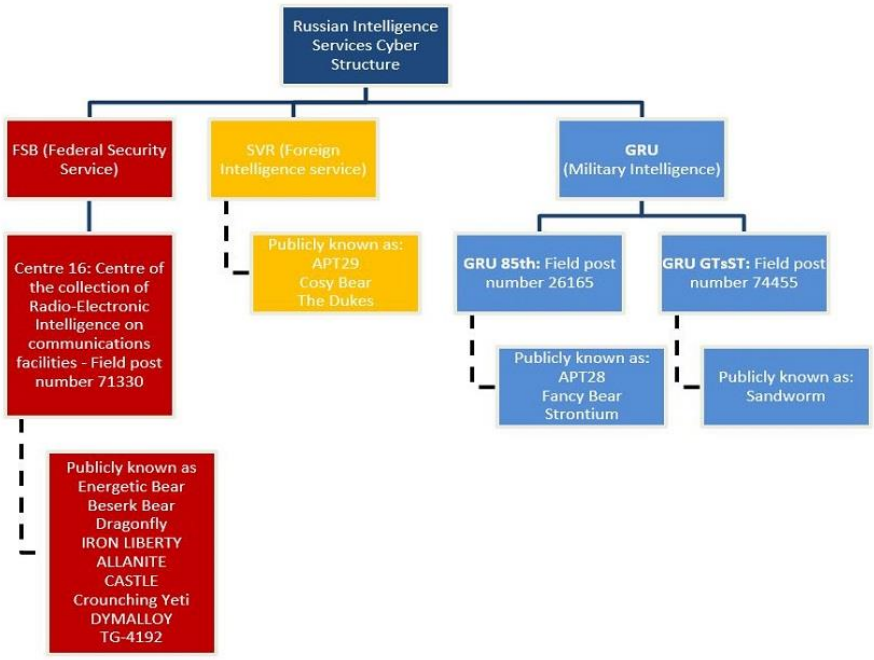

Fig.6 Russian Cyber Organogram (GOV. UK, "Cyber operations and the Russian intelligence services," 5 April 2022, (https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet))

Among these, Main Intelligence Directorate of the General Staff (Glavnoye Razvedyvatelnoye Upravleniye: GRU), the Federal Security Service (Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii: FSB) and Service of the External Reconnaissance of Russian Federation (Sluzhba vneshney razvedki Rossiyskoy Federatsii: SVR) are the three major Russian intelligence agencies, but this section discusses the FSB and GRU, which were particularly involved in the interference in the 2016 US presidential election. The FSB is a federal executive agency under the direct control of the

President. The former Soviet KGB (State Security Committee) became the Russian KGB and FSK (Federal Counterintelligence Service), which were reorganised and integrated into the current FSB in April 1995. The FSB's main responsibility and role is Russian state security. Its individual jurisdiction, as stipulated by the underlying Federal Law No. 40, includes counter-intelligence, counter-terrorism, crime fighting, information security safeguards, protection and defence of the borders of the Russian Federation, protection of the competent sea areas, territorial waters and continental shelf, exclusive economic research centres and natural resources, etc. In addition, the Centre for Electronic Surveillance of Communications (TSRRSS - Centre for Electronic Surveillance of Communications, also known as the 16th Directorate General/71330th Military Unit) has been established within the FSB and is responsible for interception, decryption and information processing of electronic communications. The centre is believed to play a central role in controlling Russian hackers. The hacker group retained by the FSB is APT29 (also known as Office Monkeys, Cozy Car, Cozy Bear and Cozy Duke), whose involvement has been pointed out in election intervention cases in various countries, as described in the previous chapters.

GRU is an internal intelligence agency of the Ministry of Defence, established in the former Soviet Union, and is the military's highest intelligence organisation, primarily responsible for the collection of military intelligence. Although organisationally it is only a branch of the General Staff within the Ministry of Defence, as in Western countries, it carries out a wide range of activities such as HUMINT, SIGINT and IMINT using 130 reconnaissance satellites, in addition to intelligence gathering through the General Staff chain, and has a special task force of 20,000 to 30,000 personnel, the Spetznaz (Spetznaz), a special task force of 20,000 to 30,000 personnel, and is also responsible for its operations, making it an intelligence organisation as powerful as the former Soviet Union's KGB (now the SVR, etc.). The hacker group under the GRU is APT28 (also known as Fancy Bear), which, like APT29, has been pointed out for its involvement in the US presidential election.

4-1-2. China

The main government agencies involved in cybersecurity in China are shown in the figure below.

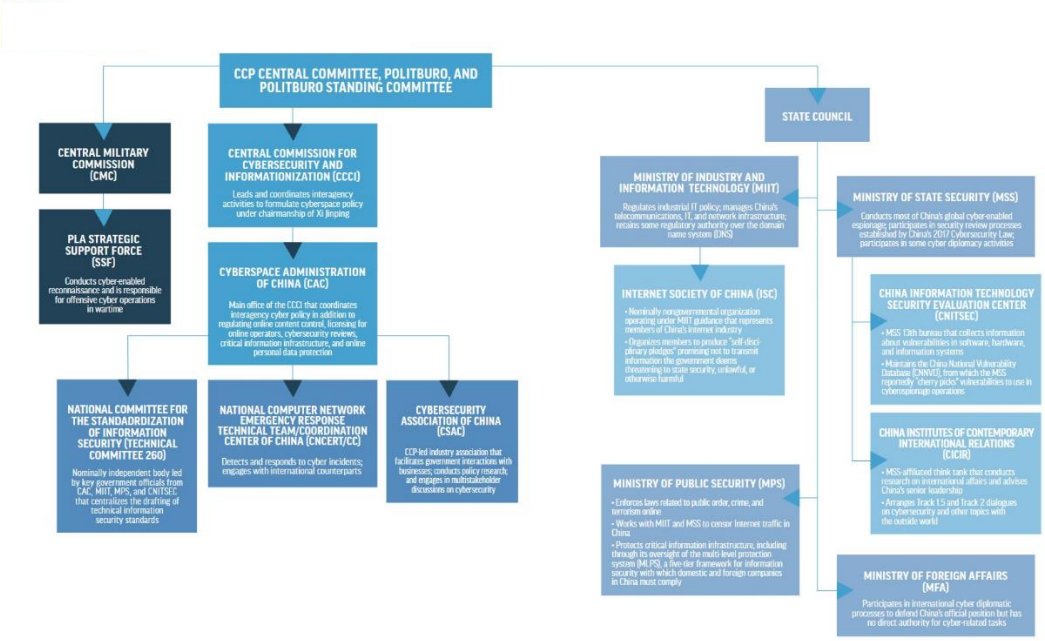

Fig.7 Selected Key Institutions in China's cybersecurity ecosystem (U.S.-China Economic and Security Review Commission, "2022 Report to Congress Executive Summary and Recommendations," November 2022. (https://www.uscc.gov/sites/default/files/2022-11/2022_Executive_Summary.pdf))

China has the President of the State as the head of the state system, but the system related to cyberspace under him can be broadly divided into two systems.

One is the Communist Party Central Cyber Security and Informatisation Guiding Group, Cyberspace Administration, State Internet Information Office, Ministry of State Security, Ministry of Public Security and Ministry of National Defence under the jurisdiction of the State Council. The other is the United General Staff and the People's Liberation Army under the jurisdiction of the Central Military Commission of the Communist Party of China.

As for the Central Cyber Security & Informatisation Guidance Group of the Communist Party, the Cyberspace Management Bureau and the State Internet Information Office, they are responsible for ensuring the security of China's cyberspace, improving information technology, training cyber personnel, drafting cyber-related policies and regulations, monitoring illegal activities, handling cyberspace-related enquiries, supporting local networks, and related industry management and international exchange, and is mainly responsible for domestic cyber security.

The Department of Public Security is positioned as China's domestic judicial police and is in charge of public security. It is responsible for crime prevention and crime investigation, traffic management, fire fighting, hazardous materials management, household registration management, immigration and foreigner management, and its main work in cyberspace is crime investigation there.

The Department of Defence, as the name suggests, is in charge of national defence, but does not

have command and control over the People's Liberation Army under the Central Military Commission, so its main role is as a military administration organ responsible for organising the army, procuring equipment, formulating training, researching and developing equipment and weapons, and liaising with foreign military counterparts. With regard to cyber, the People's Liberation Army's involvement is limited to cyber-related procurement and training formulation.

The Ministry of State Security is China's non-military intelligence agency. Its main tasks include cryptographic communications and management, collection of international strategic information, collection of political, economic, scientific and technological information of various countries, intelligence analysis and reporting, guidance of the work of competent ministries and agencies, and collection, tracking, reconnaissance and arrest of counter-espionage information. The Ministry of State Security is noted to have a hacker group APT10 (also known as 'menuPass'), which collects political-economic, scientific and technical information from various countries.[86] In addition to technical intelligence gathering, another group that is presumed to be targeted by the Ministry of State Security is what is informally referred to as the "Five Poisons". This refers to the following actors whose ideological, religious or cultural differences are labelled as poisons because they pose a direct danger to the structure of the CCP or are opposed to the government's "One China principle"[87].

・Members of the Uyghur Muslim community
・Falun Gong supporters
・Supporters of Taiwan independence
・Tibetans
・Activists in favour of Chinese democracy

Malware named 'Reaver' is often used in activities targeting them, and it has been confirmed to have been used in attacks during the 2016 Taiwan presidential election.[88]。

Among the departments related to cyber-attacks in the People's Liberation Army, the Technical Reconnaissance Bureau is the SIGINT collection and analysis organisation, with dozens of ground-based systems with long-range collection capabilities. The bureau is said to employ 130,000 linguists, technicians and researchers, although exact figures are unknown.

Then there are land and water signal units directly under the General Staff's Third Department, two bureaus in charge of the US and Canada and based in Shanghai (Unit 61398), four bureaus in charge of Japan and South Korea and based in Qingdao (Unit 61419), five bureaus in charge of Russia and based in Beijing (Unit 61565), six bureaus in charge of Taiwan and South Asia and based in Wuhan (Unit 61726) to the Shanghai-based Station 12 (Unit 61486), which intercepts communications information from space satellites and is known as the Specialised Cyber Warfare Unit. According to the report of Mandiant,[89] Unit 61398 has been linked to APT1, which conducted cyber-attacks against

the US. APT40 (also known as TEMP.Periscope), which conducted cyber-attacks and election intervention in the Cambodian general election, is also noted to be under the People's Liberation Army, although it has not been attributed to any specific unit.[90]。

4-2. The Strategy of Cognitive Warfare

As reported in Chapter 2, current information warfare has moved from cyber warfare to cognitive warfare and has taken on a complex aspect. However, the method of targeting people's perceptions itself is not new. Since ancient times, propaganda and other publicity operations have been used in warfare, but the emergence of social media such as SNS has made it easier and cheaper, and these operations have become more frequent. In the face of these trends, Russia and China have evolved their traditional strategies using new technologies and have incorporated the concept of cognitive warfare once again into their military strategies for the new era. This section provides an overview of these two countries' strategies centred on information warfare and cognitive warfare.

4-2-1. Information Confrontation-Russia

This section examines Russia's strategy in waging information warfare against the West, including Ukraine.

Russia's commitment to hybrid warfare became apparent to the Western world after the so-called Gerasimov Doctrine in 2013. This builds on Gerasimov's presentation on hybrid warfare at the Academy of Military Sciences in February 2013, in which his main themes were summarised in the paper "The value of science is in foresight (Russian: Ценность науки в предвидении)[91]". The doctrine prioritises psychological and human-centred aspects over traditional military concerns such as supplies, logistics and military strength. And it sets the ratio of military to non-military action at 1:4, emphasising a phased approach through non-military means such as information warfare and psychological warfare. (See Fig.8) According to one report[92], "the Russian view of modern warfare is based on the idea that the main battlespace is the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare, ... morally and psychologically depressing the enemy’s armed forces personnel and civil population. The main objective is to reduce the necessity for deploying hard military power to the minimum necessary."

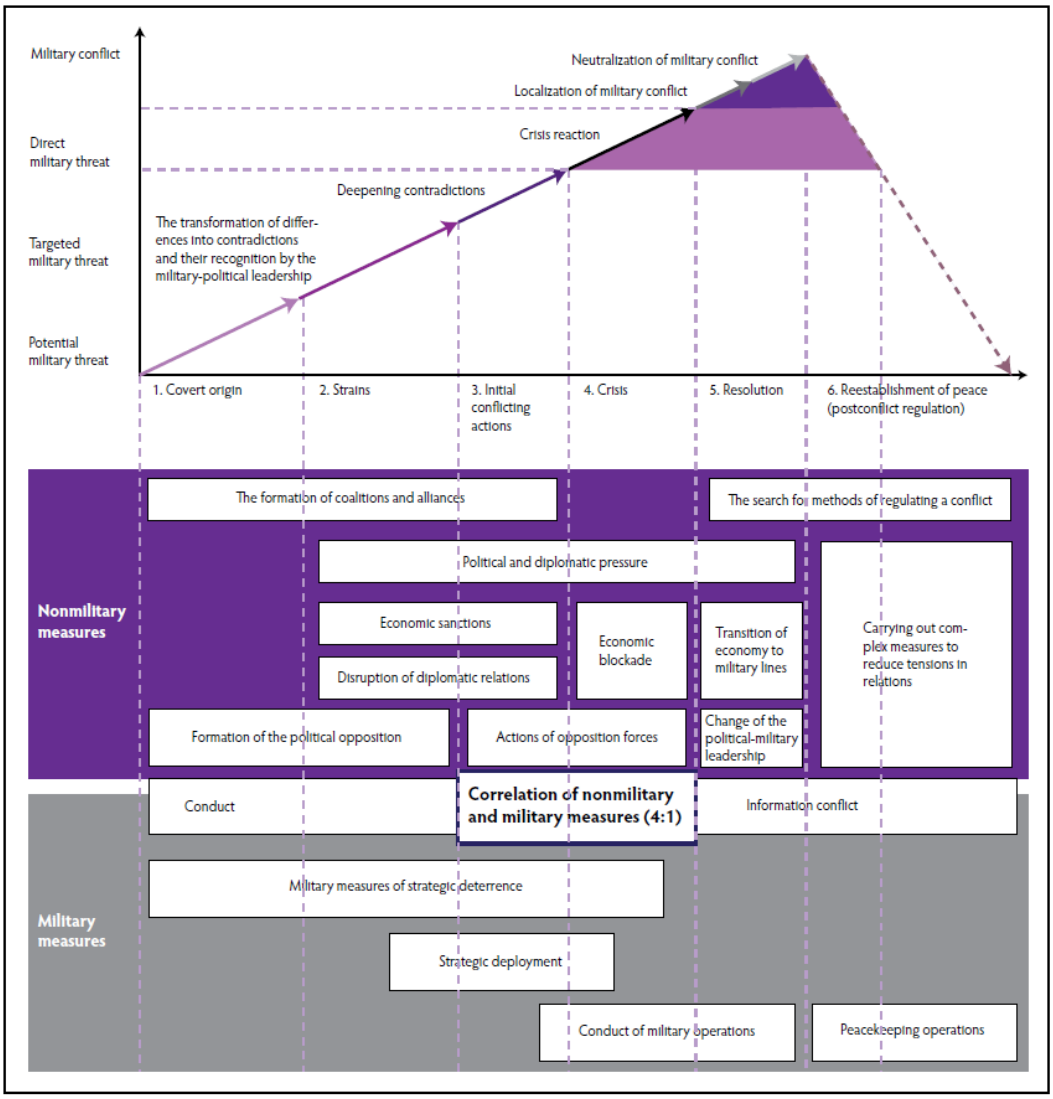

Fig.8 Graphic from Gerasimov article in Voyenno-Promyshlennyy Kurier (V. Gerasimov (R. Coalson, trans.), 2016, The Value of Science is in Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations, the Military Review. p4.))

Russia's important conceptualization of 'information confrontation' and the role of cyberspace within it is outlined in strategic policy documents, such as National Security Strategy (2015), Foreign Policy Concept (2016), Information Security Doctrine (2016), Military doctrine (2014), Conceptual Views on the Activity of the Armed Forces in the Information Space (2016), as well as works and publications by Russian military thinkers.

The analysis of NATO[93], from the Russian perspective, cyber warfare or the Russian equivalent 'information technological warfare,' is only a part of the overarching concept of "information confrontation" (informatsionnoe protivoborstvo). The Russian Ministry of Defence describes the

information confrontation as the clash of national interests and ideas, where superiority is sought by targeting the adversary's information infrastructure while protecting its own objects from similar influence. The translation of the term informatsionnoe protivoborstvo into English has proven difficult, and has often incorrectly been translated as 'information warfare' ('informacionnaja vojna'), despite the fact that protivoborstvo refers to 'counter struggle', 'countermeasure' or 'counteraction' rather than 'warfare'. This paper uses the term 'information confrontation' due to its established status in discussions regarding hostile Russian informational activities. The confrontation includes a significant psychological remit, whereby an actor attempts to affect informational resources (documents in information systems) as well as the minds of the adversary's military personnel and population at large. Ultimately, cyber operations (or information technical means) are one of many methods used to gain superiority in the information confrontation. Russia, and particularly Russian President Putin's regime, sees the information confrontation as a constant geopolitical zero-sum competition between great powers, political and economic systems, and civilizations.

Publicly available Russian doctrines and policy documents do not explicitly reference cyber operations. Furthermore, Russian documents do not use the term 'cybersecurity', but refer instead to'information security.' This term differs from the Western notion of 'Information security' in that it encompasses not only the protection of critical digital networks, but society's cognitive integrity as well.

When discussing the operational environment, Russia uses the term 'information space' (informatsionnoe prostranstvo), or 'information sphere' (informatsionnaya sfera), which again is more comprehensive than the Western concept of 'cyberspace' or'cyber domain.' The 2016 Russian Doctrine of Information Security defines the information sphere as:

"a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet […], communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating social relations in the sphere".

The information space refers to activities to form, transform, and store information, as well as 'influencing individual and public consciousness, information infrastructure and information itself. Similarly, the Russian concept of 'information weapons' (practically absent in Western parlance) includes more than just digital measures. Although the Russian Armed Forces vaguely defines them as "information technologies, means and methods used for the purposes of waging information war," in practice the concept covers a wide array of activities (often with an emphasis on affecting the human mind); this includes the spreading of disinformation, electronic warfare, the degradation of navigation support, psychological pressure, and the destruction of adversary computer capabilities.

Contrary to the Western view of interstate conflict that is based on the international legal order

outlined in international treaty and customary law (specifically the UN Charter and the Geneva Conventions) that makes a clear distinction between war and peace, Russia's 'information confrontation' is constant and ongoing. This view is exploited by Russia to undertake activities beneath the threshold of armed conflict, allowing it to remain unpredictable and pursue strategic objectives short of causing kinetic conflict. A key goal of Western democracies is to maintain a free, stable and open Internet, where fundamental rights and freedoms are ensured. In this regard, 'information security' is perceived as the protection of data and systems, but not imposing control over the attitudes and beliefs that the users of those systems are expressing. At the same time, the principles of openness and freedom of speech upheld in Western democracies might be exploited by information and cyberattacks. Russia seeks to exploit this openness to gain 'information superiority,' notwithstanding whether it is in a conventional conflict with its opponents or not.

Information warfare by Russia, is a battle to try to control the information psychological sphere of the opposing social system in order to secure this strategic advantage (information psychological warfare), and disinformation is used as a means to achieve this. There are two types of information psychological warfare: conventional warfare, which is conducted as 'maskirovka' (deception operations) to distort or conceal perceptions of specific targets, and strategic information warfare, which attempts to secure strategic superiority for the country using disinformation and other means. Russian information warfare is characterised by (1) identifying contradictions within the opponent (country or society), (2) amplifying those contradictions using fake news and other means, and (3) driving the opposing society to self-destruction through widening fissures. Russia sees the multipolarisation of the international community as an opportunity to expand its geopolitical room for manoeuvre and seeks to achieve strategic balance by weakening the West through information warfare. It seeks to magnify instabilities within the US alliance network, including the US-Japan alliance (such as the imbalances observed within the North Atlantic Treaty Organisation [NATO]), and the inherent contradictions in the democratic system, to create an opening to be exploited.

For Russia, the information space spans cognitive, cyber and physical space. Social media is an excellent vehicle for information warfare for Russia, as it spans all three spaces.

Another unique concept of Russian information warfare is "Reflexive Control," based on maskirovka, which is a Russian concept predating the Soviet Union, with the first official Maskirovka school being established in 1904[94]. Maskirovka is a concept encompassing multiple elements, such as camouflage, concealment, deception, misinformation, imitation, secrecy, security, feints, and diversion. The noun Maskirovka used to be translated as 'to mask'. First of all, this does not cover the concept at all, and furthermore it is actually impossible to translate a noun as a verb. From the original concept of Maskirovka, Reflexive Control developed to convey to an opponent specifically prepared information to incline him/her to voluntarily make the predetermined decision desired by the initiator of the action, according to one research[95]. That is, reflexive control is a sustained campaign that feeds

an opponent select information so that the opponent makes the decisions that one wants him/her to. Methods of reflexive control include spreading false information, leaking partial information at opportune moments, and projecting a different posture of oneself than what may actually be the case. The goal of reflexive control is to ‘control’ the ‘reflex’ of the opponent by creating a certain model of behavior in the system it seeks to control. It works on the opponent's 'consciousness' (long-term memory and operating memory), controls the reflex cycle consisting of 'stimulus-response' in the human cognitive domain, enters the decision-making cycle, makes the opponent perceive as if he is acting of his own free will, and guides the opponent's decision-making and reaction generation to his own advantage. This leads to decision-making and reaction generation in favour of the other party.

As shown in Fig.4 in the chapter 2, the flow of cognitive information processing in humans is not only based on sensory input, but also on the collision of information from the memory system drawn from past memories and images, which generates reactions and causes actual behaviour.

The attack on an individual's cognitive domain by disinformation does not only input false information to direct sensory inputs such as sight and hearing, but also acts on working memory (working memory) based on past memories through narratives (stories), and through cognitive filters to select and discard information. It influences the interpretation of reality (internal representation) produced within the individual's cognitive domain. As a result, they attempt to influence the individual's emotions and behaviour and elicit the given objective of the attack, which is the outcome. Such attacks on the cognitive domain have been generated from the unique Russian concept of information, as discussed above.

In the current war in Ukraine, above discussed military operational information operations (IOs) have been the mainstay of the war against Ukraine, while such cognitive warfare is mainly directed against its own country and the international community.

4-2-2. “制脑权” –China

China's strategy on hybrid warfare starts with the concept of Unrestricted Warfare (超限战/超限戰). This is warfare beyond all boundaries and limits, a concept first published in 1999 in a co-authored strategic study by Colonel 喬良 and 王湘穗 of the Chinese People's Liberation Army. Undrr the unrestricted warfare, the distinction between battlefield and non-battlefield does not exist. Natural spaces such as land, sea, air and space are also battlefields, as are social spaces such as military, political, economic, cultural and psychological. The space of technology, which connects these two major spaces, is even more so defined as a battlefield that is violently contested by the two opposing sides. And it is on the basis of this concept that the following modes of operation have been formulated. (See Table 3)

Military	Trans-Military	Non-Military
Atomic Warfare	Diplomatic Warfare	Financial Warfare
Conventional Warfare	Network Warfare	Trade Warfare
Bio-Chemical Warfare	Intelligence Warfare	Resources Warfare
Space Warfare	Psychological Warfare	Economic Aid Warfare
Electronic Warfare	Smuggling Warfare	Sanctions Warfare
Guerrilla Warfare	Drug Warfare	Regulations Warfare
Terrorist Warfare	Fabrication Warfare	Ecological Warfare
	Tactical Warfare	Ideological Warfare
	Technological Warfare	Media Warfare
		Cultural Warfare

Table 3 Forms of Unrestricted Warfare (S. Schaerer, "Chinese Espionage Against The United States," Surviving Chinese Communist Detention. (https://www.chinesecommunistdetention.com/post/chinese-espionage-in-the-united-states-military-economic-government))

This concept of Unrestricted warfare is based on the three warfare concepts of legal warfare, public opinion warfare and psychological warfare. This is based on Sun Tzu's Art of War, 「是故百戦百勝、非善之善者也。不戦而屈人之兵、善之善者也」(Winning a hundred battles is not the best of the good. (To defeat a man's army without a battle is to be the best of the good). The three concepts of warfare are: warfare, the theory of the world, and psychological warfare. This strategy was proposed in 2003 in the Political Work Regulations of the Chinese People's Liberation Army, a set of laws and regulations of the Chinese People's Liberation Army.

Legal warfare aims to ensure the legality of the use of force and operational action by one's own forces, expose the illegality of the enemy and prevent interference by third countries, thereby placing one's own forces in a position of initiative and the enemy in a position of passivity. It is used as an adjunct to military operations. Public opinion warfare refers to the cultivation of domestic and foreign opinion with the aim of inspiring the fighting spirit of one's own forces and discouraging the enemy's willingness to fight. It involves the comprehensive use of media and information resources such as newspapers, books, radio, television, the internet and e-mail. Common tactics include 'focused strikes' (to influence the decisions of the enemy leadership and others) and 'information management' (to disseminate favourable information while restricting unfavourable information). Psychological warfare aims to break the enemy's will to resist. Based on strategic intent and operational mission, it

is an operational action to influence the psychology and behaviour of an objective target through the use of specific information and media in order to realise the objectives of a political or military struggle. Regular methods of psychological warfare include offensive psychological warfare for foreign and defensive psychological warfare for domestic purposes.

Originally, physical warfare was the predominant strategy when kinetic use of force was the norm, but the transition from this to psychological warfare was only observed in 2007[96].

In the book 『从物理战到心理战』 by Professor Zeng Huaxi, Dean of the College of Humanities and Social Sciences at the National Defence University of Science and Technology, and Lecturer Shi Haiming of the Research Centre for Social Development of Science and Technology at the same university, the problems of physical warfare were pointed out and the shift to psychological warfare was advocated. The problems with physical warfare were that the targets of operations were changeable, strategic space was restricted and the cost of warfare was rising rapidly (the cost of eradication per enemy soldier during the Gulf War was $6 million). After the Gulf War, the weight of psychological warfare became heavier to overcome these factors, partly because the political and psychological goals of international public opinion became clearer with the development of mass media.

Furthermore, in 2014, in the book 『制脑权：全球媒体时代的战争法则与国家安全战略』 by Professor Zeng Huaxuan, Dean of the College of Humanities and Social Sciences at the National Defence University of Science and Technology, and Shi Haiming, Lecturer at the Centre for Research on Social Development of the National Defence University, the book "mental/ cognitive dominance (or brain control)" (制脑权). Humanity's warfare has moved from mechanised warfare into the age of informatisation, and in informatisation warfare, one must necessarily seize the initiative in warfare and the right to speak (話語権) to lead warfare. And in the information war, there are three operational spaces: natural space (land, sea, sky and sky (space)), technological space (internet space) and cognitive space (composed of human spirit and psychology). The highest state of information warfare is to deprive the opponent of "mental/cognitive dominance (or brain control)" (制脑权), which is the power of the brain formed in the cognitive space, and not to actually engage human soldiers in battle. "Mental/cognitive dominance" (mental/cognitive dominance). "The state of mental/cognitive dominance (or brain control) (制脑权) is the state of being able to secure superiority over the enemy's forces in the cognitive space and carry out various operations without significant interference from the enemy. This refers to the power to achieve control of consciousness through the use of emotions and emotional incitement.

Such operations in the cognitive space overcame the problems of physical warfare mentioned earlier. The first is borderlessness: in cognitive space, the boundaries between states and between states and individuals are blurred. There are two types of information - physical and mental - and the latter is a weapon in the cognitive space. Ideological and spiritual information can be disseminated through

language, culture and media to all the battlegrounds of cognitive space. The second is controllability, which means that information in the cognitive space of the state is manipulable. In the cognitive space, through media propaganda, certain information can be disseminated to create an image and narrative in favour of the state. Third is endurance, which means that offensive and defensive operations in the cognitive space have strategic endurance. A nation's manpower and material resources are finite and it is impossible to continue physical warfare forever, but cultural and academic exchange, public relations and media propaganda can be sustained over long periods of time.

The four methods of seizing "mental/cognitive dominance (or brain control)" (制脑权) include manipulating cognition, distorting historical memory, altering modes of thought, and attacking symbols. These are common to the structure of cognitive warfare in chapter 2 and Russian methods in the previous section.

The above description shows that both Russia and China have a concept of warfare that ranges from cyberspace to the cognitive domain as a national defence strategy. In order to formulate an appropriate defence strategy, these national strategies need to be fully analysed.

5. Limitations of International Laws

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[97], 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.

This chapter examines the issues of international law on Disinformation, both in peacetime and wartime.

5-1. Peacetime

・Rule 4. – Violation of sovereignty

A state must not conduct cyber operations that violate the sovereignty of another state.[98]

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.[99]

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[100][101][102]. 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.[103]

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.

5-2. Wartime

Rule 4 – Violation of sovereignty

A State must not conduct cyber operations that violate the sovereignty of another State

Rule 19: Circumstances precluding wrongfulness of cyber operations

The wrongfulness of an act involving cyber operations is precluded as following, consensus, self defence, countermeasure, emergency evacuation, force majeure, and distress.

Rule 20: Countermeasures

A State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State.

Rule 23: Proportionality of countermeasures

Countermeasures must be proportionate to the corresponding damage.

Rule 80: Applicability of the law of armed conflict

Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict.

Rule92: Definition of cyber attack

A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.

Rule108: Belligerent reprisals

Belligerent reprisals by way of cyber operations against:

(a) prisoners of war;

(b) interned civilians, civilians in occupied territory or otherwise in the hands of an adverse party to the conflict, and their property;

(c) those hors de combat; and

(d) medical personnel, facilities, vehicles, and equipment

are prohibited.

Firstly, cyber-attacks are defined by Rule 92 as attacks that cause injury or death to persons, damage to property or destruction, so that non-violent actions such as psychological cyber behaviour and cyber espionage do not have the character of an attack. Hence, Influence Operations are currently at the level of intensity of cyber-action. And from the Circumstances precluding wrongfulness of cyber operations as defined in Rule 19, it is understood that there is no problem in conducting counter information warfare for self-defence or countermeasures. In such a case, Rule 23 requires a balancing act whereby the same type of countermeasures can be used against violations of international law obligations. Thus, on the issue of information warfare, there is generally no illegality under international law. However, from the point of view of Rule 108, which prohibits Belligerent reprisals against prisoners of war, it can be said that acts such as Ukraine's exposure of Russian prisoners of war on social networking sites would be illegal.

However, a normative interpretation can be derived from the commentary that operations that harm the decision-making of the partner state are prohibited, as Rule 4 prohibits the violation of sovereignty through cyber operations. Currently, it is only an interpretative norm, but it is possible that it will be articulated as a separate rule in the Tallinn Manual 3.0 or later, which is currently under consideration, as a way of dealing with information warfare in the future. It could also be seen as a basis for countries to take strong action against countries conducting such malicious operations, not only through name-calling and criticism, but also through cyber counter-attacks.

Furthermore, in chapter 2, the examples of influence operations that actually resulted in physical sabotage, such as QAnon's attack on the Houses of Parliament, are mentioned, and if such operation combined with the use of force in the grey zone or in a contingency, a doctrine of accumulation of events would be applied to the the whole and could be subject to the exercise of the right of self-defence. For example, when the People's Liberation Army disguised as Chinese fishermen attempted to land on the Senkaku Islands, while at the same time satellite jamming and cyber-attacks were being carried out on Japanese communications systems, disinformation about the US military and Self-Defence Forces was disseminated in Okinawa, and mass demonstrations were agitated to disrupt the functioning of various bases. This is one of example of possible cases.

At present, international legal restrictions are loose, and domestic legal measures against influence operations are also needed. However, it should be noted that there are some arguments[104] that, in order to guarantee the credibility of a liberal democratic state, measures against influence operations should be limited to active cyber defence, platform regulation, fact checking, etc., and that the use of disinformation as a counter should not be resorted to.

5-3. International Cooperation

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”[105]) 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.

6. Countermeasures against Disinformation

6-1. Case study of countermeasures[106]

In this section, the details of countermeasures against influence operation exploiting disinformation are reviewed.

6-1-1. US

(1-1) Agencies and systems to detect and monitor disinformation

In May 2018, the Department of Homeland Security (DHS) established the Countering Foreign Influence Task Force (CFITF) was established. Subsequently, in November 2018, following the bipartisan Congressional passage of the Cybersecurity and Infrastructure Security Agency (CISA) Establishment Act, the NPPD was transformed into CISA and the CFITF became part of CISA. the CFITF is responsible for the management of the National Security and Infrastructure Security Agency's (NSPA) cybersecurity and infrastructure security operations, including the countering of Mis-, Dis- and Mal- information), and was given the specific mandate to promote the understanding of the US public regarding the risks and effects of MDM.

In 2021, the CFITF was reorganised into CISA's MDM Team, whose current role includes collecting information on MDM, analysing it and publishing fact-check results. the MDM team is responsible for building national resilience against malicious MDM activity through interagency and private sector It works closely with partners, social media companies, academia and international partners, and is also responsible for coordinating.

(1-2) Investigating and punishing election interference

In September 2018, President Trump signed Executive Order 13848, which imposes sanctions against interference by foreign governments and others in US elections (at the federal level). Within 45 days of the election results, the Director of National Intelligence will investigate whether there was interference in the election in question, and within 45 days thereafter, the Attorney General and the Secretary of Homeland Security will decide whether to impose sanctions. Sanctioned persons will have their assets in the US frozen and will be prohibited from doing business with US persons.

In the 2018 midterm elections, the investigations did not confirm any vote interference or tally tampering, and as indicated in the previous chapter, the decision was that although influence operations by Russia, China and Iran were confirmed, their impact on the election results was not assessed. On the other hand, the study assessed Russian and Iranian influence operations in the 2020 presidential elections. As for China, the report states that it did not carry out such operations in view of US-China relations, although a minority opinion notes that there were some sabotage attempts. However, it was assessed that there was no evidence of any specific influence of foreign governments on the voting process or the outcome of the US presidential election itself in any of the operations carried out by

any of the countries.

At the state legislative level in the US states, in September 2019, Texas passed a law making it a misdemeanour to produce and share political deepfakes (elaborate AI-based fake videos) distorting facts about political opponents one month before an election. In October of the same year, California also passed legislation making it illegal to create or distribute falsified videos, audio or photographs of election candidates. Deepfakes influencing elections are also beginning to be recognised as punishable offences.

(2) The designation of election as critical infrastructure

On 6 January 2017, DHS designated elections as one of the 'critical infrastructures' (Critical Infrastructure) under The Patriot Act of 2001, which was passed in response to the 2001 terrorist attacks. The Department of Homeland Security (DHS) defines critical infrastructure as 'assets, systems and networks whose incapacitation or destruction is believed to undermine the security, economy, or national health or safety of the United States' and has designated 16 areas for focused protection. There is an agency responsible for each area, such as the transport system, the defence industrial base and financial services, while election infrastructure is the responsibility of DHS and is designated as a subsector in the 'Government Facility' area (Election Infrastructure Subsector). This allows DHS to provide support to election authorities when requested, to liaise with other intelligence agencies such as the Office of the Director of National Intelligence (ODNI), and to share information on cyber threats, vulnerabilities and incidents (incidents that could lead to accidents) through the establishment of Election ISACs. The establishment of the Election ISAC has also led to the sharing of information on cyber threats, vulnerabilities and incidents.

(3) Active cyber defence

In the days following 6 November 2018, when the US midterm elections took place, USCYBERCOM blocked internet access by the Russian IRA. As previously mentioned in the previous chapter, the IRA is a company that is alleged to have interfered in the 2016 US presidential election and other elections through disinformation activities and has been linked to the Russian Government. In addition, USCYBERCOM did not merely block access, but also carried out operations such as sending warning messages to the other party regarding the cyber-attack.

In March 2021, USCYBERCOM commander Paul Nakasone told a Senate Armed Services Committee hearing that the company had conducted more than two dozen operations to pre-empt interference or obstruction by foreign powers in the 2020 US presidential election[107]. The actual nature of the operations has not been disclosed, but it was clearly stated that the operations targeted hostile forces in Russia, Iran and China, and as with the 2018 midterm elections, it is believed that the operations were hackers' attributions for foreign powers' interference behaviour, tactical understanding

and countermeasures against their opponents.

(4) Platform regulation.

In October 2017, the Honest Ads Act, an online advertising regulation bill, was introduced by three bipartisan members of Congress. The bill requires platform operators with more than 50 million monthly visitors to record and disclose details such as content, subject matter, number of views, advertising fees and advertisers of political advertisements paid for at least $500 per year, as well as preventing the purchase of foreign political advertising for the purpose of influencing US voters Requires measures to be taken to prevent the purchase of political ads from foreign countries for the purpose of influencing US voters; Facebook announced its support for the Act in April 2018 and it was introduced in the US Senate Congress in 2019, but the bill failed to pass.

On 31 October 2017, the US Senate Judiciary Committee's Subcommittee on Crime and Terrorism held a hearing on the allegations of Russian meddling in the 2016 US presidential election, inviting the General Counsel of Facebook, Twitter and Google to testify and answer questions. Also on 5 September 2018, the US Senate Intelligence Committee invited the CEOs of Facebook, Twitter and Google to testify before the US Senate Intelligence Committee on the recent foreign (mainly Russian) influence on social networking and the transparency and responsibility of their services. Thus, in the US, each platformer has been called to congressional hearings and required to be accountable.

In addition, as of January 2022, there are various developments surrounding amendments to Section 230 of the Communications Decency Act of 1996 (CDA, hereafter referred to as the Communications Decency Act). Section 230 provides that platform companies are immune from liability for the content they transmit on online platforms. In June 2019, an amendment to the article was proposed by a Republican senator . The amendment requires platform operators above a certain size to obtain certification from the Federal Trade Commission that they have not coordinated user-submitted information in a politically biased manner as a requirement for receiving immunity for user-submitted information and its editing or deletion. This was criticised at the time by user and industry groups on the grounds that leaving the determination of political bias to government agencies could curtail freedom of expression.

In May 2020, President Trump issued Executive Order 13925, which changed the interpretation and enforcement of the article, naming Twitter, Facebook, Instagram and YouTube, and clarifying the scope of platformers' responsibilities and imposing them on par with traditional editors and publishers It called for the same. This led to a move to amend the Article, and in October 2020, Republicans and Democrats agreed to reconsider the Article, and hearings were held by the Senate Committee on Commerce, Science and Transportation and the Judiciary Committee, which held hearings for the CEOs of Twitter, Google and Facebook respectively. At these hearings, the companies agreed to be more transparent about their surveillance; in 2021, a change of government resulted in the Joe Biden

administration, but President Biden has stated that the Article should be repealed immediately, and it is likely that the amendment will continue to move forward.

(5-1) Media literacy education

In April 2017, Washington State passed a law promoting media literacy education and safe internet use. Under the Act, media literacy education in school education is being investigated and reviewed. Similar legislation has been passed in California, Connecticut, Rhode Island and New Mexico, and bills have been introduced and are being discussed in 19 other states. The background to these is that Media Literacy Now, a private organisation that promotes media literacy education, is encouraging the enactment of similar legislation by preparing and publishing model bills.

(5-2) Fact-checking Organisation

According to the database of fact-checking websites created and published by the Duke Reporters' Lab at Duke University in the United States, there are a number of fact-checking organisations in the United States that meet certain standards[108]. The government itself has also developed its own fact-checking system.

The government itself also has a fact-checking function, and CISA's MDM team, mentioned above, has established a website called 'Rumor Control[109]' to disseminate fact-checking information.

6-1-2. UK

(1-1) Institutions and systems to detect and monitor disinformation

In January 2018, the UK Government announced the establishment of a task force in the Cabinet Office, the National Security Communications Unit, to combat disinformation activities by foreign powers. The task force will be responsible for monitoring, analysing and evaluating the activities of foreign powers in cyberspace, as well as coordinating with other ministries and international organisations. A Rapid Response Unit (RRU) has also been set up in conjunction with the taskforce to specifically monitor social networking services, with a team of data scientists and media experts monitoring social networking services 24 hours a day. The RRU detects, analyses and assesses disinformation and misinformation circulating on social networking sites.

(1-2) Investigation and punishment of election interference

The UK has not yet developed legislation to investigate and punish disinformation campaigns by foreign powers, as is the case in the US. However, in January 2017, the House of Commons Digital, Socialisation, Media and Sport (DCMS) Select Committee launched an investigation into the impact of fake news on democracy, publishing an interim report[110] in July 2018 and a final report[111] in February 2019. The report discloses how much research the Government has conducted so far into the

2014 Scottish referendum, the 2016 UK referendum and the 2017 UK general election, and calls for it to conduct its own research again. In addition, it has recommended that stiffer penalties should be prescribed for users who misuse social networking and other information systems for the purpose of manipulating information, and it is anticipated that such legislation will be introduced in the future.

(2) Designation of elections as critical infrastructure

As of November 2022, elections have not been designated as critical infrastructure.

(3) Active Cyber Defence

As of November 2022, cyber counter-attack legislation targeting disinformation is not in place. However, the interview[112] of the UK Defence Minister Ben Wallace revealed that the UK Ministry of Defence is planning to establish a Digital Warfare Centre with a cyber counter-attack capability of several thousand people to conduct cyber counter-attacks against cyber-attacks and disinformation from hostile states.

(4) Platform regulation.

The DCMS final report mentioned above also makes recommendations on the development of a code of ethics, the establishment, monitoring and enforcement of an independent regulatory body for platformer companies, and charging and taxing platformers. In response, the UK Government has announced that a new dedicated organisation to monitor and regulate platformers will be established within the Competition and Markets Authority (CMA), the equivalent of Japan's Fair Trade Commission, and that a Digital Marketing Unit (DMU) will be launched within the CMA in April 2021. The DMU will have various legal powers, such as injunctions and corrective action orders against platform companies, including Google and Facebook, on which digital advertising is based, if they are deemed to be problematic in terms of fair market competition. Specifically, the CMA will develop legal rules requiring greater transparency in the handling of services and user data; the CMA has also noted the use of information provided by the press by platform companies without payment, and will also oversee the content of contracts for the use of articles to ensure that news organisations receive fair compensation. .

(5-1) Media literacy education

The DCMS final report above recommends initiatives to improve the public's information literacy. In addition, in June 2018, the Fake News and Critical Literacy Education Committee, a bipartisan group in the UK Parliament, released its final report entitled 'Fake News and Critical Literacy', which stressed the need for critical literacy cultivation to counter fake news. In light of this situation, a curriculum to counter fake news was introduced in school education from 2020 as a joint initiative of the Ministry

of Education and the Ministry of Health.

In addition, the Government Communication Service's (GCS) new programme, the Accelerate Programme, has introduced a media officer using the FACT model to detect and assess disinformation and misinformation used by RRUs. The Accelerate Programme is developing bespoke training for media officers using the FACT model to detect and assess disinformation and misinformation used by RRUs. This includes a series of secondments to RRUs for training. These initiatives show a commitment to educate and train the senders as well as the recipients of information.

(5-2) Fact-checking organisations

In the UK, seven fact-checking websites are operated, mainly by media organisations such as the BBC, Channel 4, Reuters and the Guardian. Full Fact, run by a charity based on private donations, has secured funding from Google and developed a tool called LIVE AND TRENDS that automatically fact-checks from TV subtitles and other real-time information sources[113].

6-1-3. Germany

(1-1) Agencies and systems to detect and monitor disinformation.

As of November 2022, there is no institution in Germany that monitors disinformation on a permanent basis. However, in the new Cyber Security Strategy approved on 8 September 2021 and the Federal Election IT Security Plan developed on the basis of the Strategy, the Federal Information Security Agency (Bundesamt für Sicherheit in der Informationstechnik: BSI) was was designated as the competent authority. In the Agency, a department was set up to intervene in social networking sites during the election period by notifying the corresponding social media providers when automated bots or coordinated fraudulent activities were detected. The Federal Election Commission is also responsible for identifying and addressing disinformation related to the overall electoral process, and publishes the information it identifies through its fact-checking website.

(1-2) Investigation and punishment of election interference.

In Germany, measures are mainly focused on platform regulation, which will be discussed below, and even during the election period, the above-mentioned monitoring investigations are limited to the election period. At present, there is no post-sanction legislation to investigate and punish the disinformation activities of foreign forces.

(2) Designation of elections as critical infrastructure.

As of November 2022, elections have not been designated as critical infrastructure.

(3) Active cyber defence

As of November 2022, there is no legislation in place for cyber counter-attacks targeting disinformation.

(4) Platform regulation.

In June 2018, Germany passed a law (SNS Enforcement Act [Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerke: NetzDG]) to improve law enforcement on SNS. SNS operators with more than 2 million registered users in the country are subject to the law, and the subject operators are obliged to set up a window air strip for reporting content that is illegal under the Criminal Code, immediately examine the illegality if a report is received, and delete or block access within a prescribed period (within 24 hours or 7 days depending on the degree of illegality). Obligation. Subject operators who receive more than 100 complaints about illegal content per year are obliged to prepare a complaint-handling report covering the period in question every six months and publish it in the Federal Official Gazette and on their own websites. Non-compliance with these is subject to a fine of up to EUR 50 million.

In July 2019, the judicial authorities ordered Facebook to pay a fine of EUR 2 million for deficiencies in the report on deletion cases it submitted, including the fact that only some of the cases were mentioned; until 2020, this was the only case in which a fine was imposed under the Act[114]. The law has raised concerns about 'overblocking', in which it is difficult to understand the criteria for content to be removed and internet operators excessively restrict the content they publish. In response to this situation, the SNS Enforcement Act was also amended in the same year to encompass the Bill on Right-wing Extremism and Hate Crime, which was passed in June 2020, and clarifies the process for filing complaints about illegal content, as well as the obligation to report removed offending content to the Federal Criminal Agency (Bundeskriminalamt : BKA) on the offending content that has been removed. In addition, in order to increase transparency, the operators' reports were amended in the direction of stricter regulations overall, with the added obligation to report whether automatic content detection algorithms for illegal content are used and, if so, how they work.

(5-1) Media literacy education

EU-sponsored media literacy education project for young people and older people by the German private foundation Stiftung Digitale Chancen (Digital Opportunities Foundation) under the auspices of the Federal Ministry for Economic Affairs and Energy and the Federal Ministry for Family, Ageing, Women and Youth "Get your facts straight![115]" as a partner organisation to raise awareness in Germany. The BSI also conducts media literacy education campaigns for politicians at election time, and raises awareness on how to increase the safety of social network accounts of candidates and election officials, for example by producing a security guide[116].

(5-2) Fact-checking organisations

As mentioned in (1-1) above, information on the correction of disinformation identified by the Federal Election Commission is made public through the fact-checking website[117]. In the private sector, six fact-checking websites are operated, mainly by broadcasters and media organisations of regional origin, such as Second German Television (ZDF).

6-1-4. France

(1-1) Institutions and systems to detect and monitor disinformation

In June 2021, the French Government announced plans to establish an agency to counter foreign disinformation and fake news aimed at 'undermining the State' (Viginum: Le service de vigilance et de protection contre les ingérences numériques étrangères), which aims to 'combat foreign disinformation and fake news'. This was intended as a countermeasure to the forthcoming presidential elections in April 2022. The agency was established under the General Directorate of Defence and Security (SGDSN) by decree in July 2021 and became operational on 15 October of the same year. The agency's mandate, according to the Director General of the SGDSN, is to 'monitor, detect and characterise foreign digital interference activities aimed at manipulating information on social networks' and 'never to certify the authenticity of information'. The certification of the authenticity of information is carved out as a role for politicians, the media and the judiciary, and the agency's activities are reviewed by an ethics committee made up of parliamentary, judicial, diplomatic, media and research officials.

(1-2) Investigation and punishment of election interference.

In France, there is no legislation on ex-post sanction-type investigations and punishments, as in the United States. However, in the report[118] in 2018 by the Ministry of Foreign Affairs and the Strategic Research Institute of the Military Academy (L' Institut de recherche stratégique de l'École militaire: IRSEM), entitled 'Information operations - a challenge to our democracy', the report urged the Government to Citing the example of US Special Prosecutor Robert Mueller's prosecution of Russian officials and Russian-related entities in the 2016 US presidential election, the report recommends that those responsible for serious interference during the election period and elsewhere should be punished. Specifically, it mentions punishing those responsible for serious interference in the electoral process, etc., through economic sanctions or legal proceedings if the responsibility can be clearly identified, and it is likely that legislation similar to the US ex-post sanctions type will be developed in the future.

(2) Designation of elections as critical infrastructure.

As of November 2022, elections have not been designated as critical infrastructure.

(3) Active cyber defence

As of November 2022, there is no legislation in place for cyber counter-attacks targeting disinformation.

(4) Platform regulation.

In November 2018, a law on combating disinformation was passed. During the election period, courts may order anti-transmission measures if information is disseminated that fits the stipulated definition of fake news. Platforms are also obliged to cooperate in disclosing the source of funding for article body advertising (sponsored content) and the originating entity, anti-bot measures and literacy education, etc. As for television and radio, if media outlets with foreign management rights report fake news, the media regulatory body can order them to stop broadcasting The media regulator can order them to stop broadcasting.

(5-1) Media literacy education

In the report, 'Information Manipulation - A Challenge to Our Democracy', the Government has recommended that media literacy education should be provided not only to young people but also to adults as well.

Since 2015, the French Government has increased funding for educational courses on improving media literacy online, with some 30,000 teachers and other education professionals receiving government training on the subject each year. The French Ministry of Culture doubled the annual budget for the course to EUR 6 million (USD 6.8 million) in 2018, double the previous budget, while the Ministry of Education added a similar high school course to the national curriculum as an elective subject, making it available to thousands of people via the internet and other media. In the same year, the Government also established a new secondary school course in cooperation with journalists and educators. In addition, some local authorities are working to improve media literacy education across the country, for example by requiring young adults to have completed an internet literacy course when they receive monthly benefits and other benefits.

(5-2) Fact-checking organisations.

In France, 17 fact-checking websites are operated, mainly by media organisations such as AFP and Le Monde, and fact-checking websites dedicated to climate and immigration issues are also available.

6-1-5. EU

(1-1) Institutions and systems to detect and monitor disinformation interference

The Strategic Communications Task Force (East StratCom Task Force) was established in March 2015 as part of the EU Action Plan on Strategic Communications to address Russian disinformation

campaigns. The Task Force is part of the Strategic Communication and Information Analysis Division (AFFGEN.7) of the European External Action Service (EEAS), which includes the EU's Rapid Alert System on Disinformation), as well as a coordination team focused on international cooperation. The Strategic Communications Task Force has a wide range of activities, including disinformation trend analysis and reporting, clarification of disinformation narratives, literacy education aimed at raising public awareness of the threat of disinformation, and international cooperation for information sharing. As of March 2021, it had 16 full-time staff and a budget of EUR 11 million.

(1-2) Investigation and punishment of election interference

The EU as a whole, mainly led by the European Commission, was early on considering measures to counter Russian disinformation with regard to election interference: a High-Level Expert Group (HLEG) was set up in November 2017 and a report by the HLEG was published in the following March 2018. Based on that report, a European Commission statement on countering fake news was published in April, and a Code of Conduct on Disinformation was developed based on this statement. The Code aims to improve transparency and ensure cyber hygiene in social networking and web media, and requires platforms that have agreed to the Code of Conduct to implement it.

Against this background, the European democracy action plan[119] was published in December 2020. The plan also explicitly states that one of its objectives is to impose costs on perpetrators of disinformation, and states that it will strengthen task forces and provide capacity-building support to promote monitoring and investigation of disinformation activities in the region. While the direction of imposing sanctions on perpetrators is indicated, the details of these sanctions have not been clarified.

(2) Designation of elections as critical infrastructure.

As of November 2022, there is no EU-wide system to designate elections as critical infrastructure. However, in 2019, the European Union Agency for Cybersecurity (ENISA) will require Member States to classify their electoral systems, electoral processes and electoral infrastructure as critical infrastructure and to implement the necessary cybersecurity measures[120].

(3) Active cyber defence

As of November 2022, there is no legislation in place for cyber counter-attack targeting disinformation.

(4) Platform regulation

The EU has been working on platformer regulation since early on. The Code of Conduct to date has focused on platformer self-regulation, requiring platformers who have agreed to the Code of Conduct to (i) scrutinise the content of their advertisements and the source of their funding, (ii) work to increase

transparency in advertising based on political issues, and (iii) report regularly on the status of their implementation. The Code of Conduct was then strengthened by the European Democracy Action Plan in December 2020, which resulted in the publication of the Guidance on Strengthening the Code of Conduct on Disinformation in May 2021. The 'Guidance' establishes the Digital Services Act, which provides for a move towards a co-regulatory regime with platforms; the expansion of signatories to include private messaging service providers; a strengthened commitment to achieving the objectives of the Code; a robust monitoring framework, including clear key performance indicators for the delivery of the Code; a standardised format, classified by Member State, for reports, the establishment of a transparency centre and a permanent task force to evolve and adapt the Code.

The Commission has also proposed legislation on transparency of sponsored political content.

(5-1) Media literacy education

The above-mentioned European Democracy Action Plan provides for media literacy education to combat disinformation, in conjunction with the New Digital Education Action Plan (2021-2027) The New Digital Education Action Plan includes the development of common guidelines for teachers and educational staff, collaboration with different stakeholders such as telecommunications operators, journalists and the European Digital Media Observatory (EDMO) The plan also provides directions for collaboration with various stakeholders, such as telecommunications operators, journalists and the European Digital Media Observatory (EDMO), as well as financial support for educational and research organisations to promote digital education.

(5-2) Fact-checking organisations

The EU-wide fact-checking organisations are EU vs Disinfo and EU factcheck. The former publishes information monitored and verified by the Strategic Communication Task Force. Although not independent of the executive branch, it publishes a systematic database of disinformation, mainly on Russia, and provides useful analysis. The latter is a private sector-based fact-checking organisation based on the European Journalism Training Association (EJTA).

6-1-6. Singapore

(1-1) Institutions and systems to detect and monitor disinformation.

In October 2021, the Foreign Interference [Countermeasures] Act (Fica) was passed by the Singapore Parliament. The Act aims to introduce countermeasures to prevent, detect and hinder Hostile Information Campaigns (HIC) by hostile foreign powers and interference in domestic politics conducted through domestic agents deemed politically significant.

According to Singapore's Ministry of Home Affairs, HIC aims to influence domestic political discourse, incite social discord and undermine political sovereignty, using sophisticated online tools

and tactics as a way to promote foreign interests. Therefore, if there is a suspicion that HIC content is occurring, the Home Secretary can order preventative measures to be taken on social media services, related electronic services, internet access services, etc., and the Ministry of the Interior has the power to investigate HIC for this purpose.

(1-2) Investigation and punishment of election interference

The above-mentioned Foreign Interference Prevention Act is not limited to election periods, but defines individuals and non-individuals directly involved in Singapore's political process as Politically Significant Persons (PSPs) and provides for measures to reduce the risk of foreign interference. It states that measures will be taken to reduce the risk of foreign interference, and measures against electoral interference are also considered.

PSPs cover political parties, persons in key political positions, members of parliament, parliamentary leaders, leaders of opposition parties, election candidates and their election agents. In addition, other individuals and organisations that are vulnerable to foreign interference may also be designated as PSPs by the relevant competent authority designated by the Minister of the Interior, if their activities are directed towards political objectives. Individuals and organisations designated as PSPs may be subject to foreign influence if they They are obliged to disclose if they receive donations that could be considered to be of foreign influence, or if they are asked to disclose the affiliations of those involved as volunteers or members.

Measures such as blocking access to websites and other sites suspected of being involved in HIC, or blocking advertising revenues after identifying them as prohibited sites, are taken; for PSPs, the offence of publishing information online without declaring foreign involvement (or the intention to do so) is punishable by imprisonment of up to 14 years and a fine of S$100,000 for individuals and S$1 million for legal entities such as news websites.

(2) Designation of elections as critical infrastructure.

As of November 2022, elections have not been designated as critical infrastructure.

(3) Active cyber defence

As of November 2022, there is no legislation in place for cyber counter-attack targeting disinformation.

(4) Platform regulation.

In October 2019, the Prevention of Fake News Act (POFMA), commonly known as the Prevention of Fake News Act (POFMA), came into force with a view to countering false information in the following general election in July 2020. The Act prohibits the dissemination of information that meets

the following requirements: i) information that is identified by the Government as false; ii) information that could threaten national security or public welfare and is deemed to incite hostility or hatred between groups; iii) disinformation that could affect the outcome of the election; iv) disinformation that could undermine public confidence in the Government's ability to perform its duties. (iii) misinformation that could potentially undermine public confidence in the government's ability to carry out its duties.

Section 7 of the Act also prohibits an individual from knowingly communicating (e.g. retweeting) a false statement that.

・Discourses that may adversely affect the security of Singapore.
・Discourses that are likely to adversely affect public health, public safety or financial stability
・Discourse that may adversely affect the friendly relations between Singapore and other countries.
・Discourses that may affect the outcome of presidential, general, by-elections, by-elections or referendums.
・Discourses that may incite hostility or hatred between different groups of people.
・Discourses that is likely to reduce public confidence in the duties, functions and enforcement of government institutions.

Individuals who contravene Section 7 are liable to a fine of up to S$50,000 and/or imprisonment for up to five years. Non-individuals, for example, online media platforms operated by high-tech companies, face fines of up to S$500,000. Individual offenders are also liable to a fine of up to S$100,000 and/or imprisonment for up to 10 years if they use fake online accounts or bots to spread such falsehoods. Non-individuals are liable to a fine of up to S$1 million.

Section 3 of the Act provides that a communication subject to POFMA may be made via the internet, social media such as Facebook and Twitter, multimedia messaging services (MMS) and short message services (SMS) to It defines a communication as a discourse communicated to one or more end-users in Singapore. Senior Minister for Law Edwin Tong clarified in Parliament that the POFMA also covers closed platforms such as private chat groups and social media groups.

The Singapore Government may order anyone who disseminates information that contravenes the Act to remove such information, stop posting it and post a correction stating that the information is incorrect. The Government also has the power to order companies providing social networking platforms to communicate to their users that the information concerned was false. The government has the authority to identify fake news and can issue instructions to the internet intermediary that posted the information, requiring it to suspend service to the target account or prohibit it from interacting with other users.

The content and corrections will be posted on the Singapore Government's websites “Factually”[121],

but a link to the Government's site must be attached to any web representation that the information is false.
Examples of law enforcement against platformers and others under the Act as follows.

・In November 2019, the Singapore Government instructed Facebook to correct a post accusing it of election fraud under POFMA; Facebook posted a 'correction notice' at the end of the corrected post, while also urging the country's Government to carefully enforce the new law. It urged the government to carefully implement the new law.
・In January 2020, a Malaysian human rights group posted on Facebook that the Singaporean Government had "not accepted" the statement that "prison officers in Singapore are trained in cruel execution methods in case the rope breaks during executions" and that the Singaporean Government had "not accepted" the statement and ordered the human rights group and the website that spread the claim. The Singaporean Government ordered the human rights group and the website that spread the claims to correct them, and ordered the operator to block access to the human rights group's website from the country.
・In July 2020, in response to claims posted on Facebook by the opposition party People's Voice and on YouTube by the leader of the Lim Teen Party that the opposition party and the leader of the Teen Party were "spending large amounts of money to provide free educational opportunities to foreigners", the Singapore Government issued correction orders to the Opposition and Teen Party Leader under POFMA.
・In August 2021, in response to a posting on a noticeboard on a website run by a local media giant claiming that there had been deaths from a new virus in the country, the Singapore Government denied the claim and ordered the operator of the board to correct it.
・In October 2021, Singapore health authorities announced that they would apply POFMA and pursue a criminal investigation against the website Truth Warriors, which claimed that the vaccine for the new corona was unsafe. Through a statement, the Singapore Health Authority noted that the information was "all unverified false material" and "puts the website's visitors at risk", and ordered that "having decided to apply POFMA, the website must post a notice to its readers that it contains 'false facts about the content'". The order stated that "the website must publish a notice to its readers that it contains 'false facts about its content'".

With regard to the operation of POFMA, criticism has arisen that it could lead to the suppression of speech, as the Government has the power to certify that certain information is false or 'fake news' under the Act.

(5-1) Media literacy education

In January 2019, the Minister of Culture, Social Affairs and Youth announced the launch of two new initiatives[122]: a seminar entitled 'Fighting Fake News' for religious and social organisations in the country and the production and distribution of an advisory book on security .

(5-2) Fact-checking organisations.

Singapore accepts reports of potentially false information in accordance with the provisions of the POFMA. Based on such reports, the government publishes the results of fact-checking on the website Factually for information that it identifies as false. In addition, two fact-checking websites are operated in the private sector, mainly by media organisations such as AFP.

6-1-7. Taiwan

(1-1) Institutions and systems to detect and monitor disinformation

By the end of 2019, Taiwan has deployed Meme Engineering teams (迷因工程團隊) in all ministries and agencies under the leadership of Political Affairs Commissioner for Digital Affairs Audrey Tan to monitor social networking and disseminate fact-checking results. The Executive Yuan has adopted the '2-2-2 principle', which requires that if a ministry team discovers disinformation or misinformation, it must publish a correct explanation for the information on the SNS within 20 minutes, 200 characters or less and with two images.

(1-2) Investigation and punishment of election interference

In December 2019, the Anti-Intrusion Act was passed to prevent extraterritorial hostile forces from intervening in Taiwan, and came into effect the following January 2020. The law prohibits political donations under the direction, commission or funding of extraterritorial hostile forces, electioneering, spreading disinformation and obstructing legitimate demonstrations. Violations of the Act can result in imprisonment for up to five years and a fine of up to TWD 5 million (approximately NTD 18 million). The Act does not only target disinformation campaigns by foreign forces, but also aims to prevent political intervention in Taiwan by foreign forces themselves.

(2) Designation of elections as critical infrastructure.

As of November 2022, elections have not been designated as critical infrastructure.

(3) Active cyber defence

As of November 2022, there is no legislation in place for cyber counter-attack targeting disinformation.

(4) Platform regulation.

Taiwan's policy on cracking down on fake news and other forms of news on social networking sites is not oriented towards regulating platformers, but only towards regulating and punishing the originators of fake news. Seven laws, including the Disaster Prevention and Relief Act and the Radio and Television Act (廣播電視法), have been amended to prevent fake news, and in the Social Order Maintenance Act, a provision on the spread of rumours has been added, expanding the scope to include fake news and strengthening penalties such as fines and detention. Furthermore, ministers have commented that they are considering amending the law to include fines for social networking platforms that fail to remove fake news, and it is expected that the law will be amended in this direction in the future.

(5-1) Media literacy education

In Taiwan, the Government has established a cooperative relationship with Facebook, Google and LINE in media literacy education, and the three companies are funding educational programmes for this purpose.

(5-2) Fact-checking organisations

In Taiwan, four organisations and websites are active, led by the Taiwan Fact Check Centre, which was jointly set up by the Taiwan Media Watch Foundation (TAIWAN MEDIA WATCH) and the Superior Quality Newspaper Development Association (weReport). Communication tools such as LINE and chatbots are also actively utilised[123].

In addition, as mentioned above, ministries and agencies are working on disseminating fact-checking based on the 2-2-2 principle. In this measure, the 'humour over rumor' strategy is adopted to ensure that accurate information is disseminated more widely and faster than fake news, being aware that fake news and misinformation spread faster because of their sensational content. strategy' to ensure that accurate information spreads faster than fake news. The strategy uses a technique called 'meme engineering', in which humorous content, such as mascot characters and comical images, is transmitted together with commentary on the fact-checking results.

6-2. Types of Legal Challenges

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 of the Poynter Institute[124], 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 4 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.

7. The Evaluation Model for Nations against Disinformation

7-1. Evaluation Model

Based on the previous discussions, this chapter presents and discusses an evaluation model of the national strategies that each country should take as a countermeasure against disinformation. The model divides the areas to be considered as strategies into six broad categories and quantifies the achievements in each area to assess the state of achievement and balance. As a result, it can be clearly shown that Japan is significantly behind in the state of countermeasures, and by identifying Japan's challenges, it will be connected to policy recommendations on events.

In constructing this evaluation model, reference was made to existing indicators of national cybersecurity efforts. Typical of these indicators are the Global Cybersecurity Index (hereafter "GCI") created in 2014 by the Cybersecurity Team of the Inter- national Telecommunication Union (ITU)[125] and the Cybersecurity Capacity Maturity Model for Nations Revised Edition (hereafter “CSCMMN”)[126]. GCI is a questionnaire-based index in which Member States answer and score 157 questions in five areas - legal, technical, organisational, capacity development and cooperation. However, the questions do not take into account the process of legal and regulatory reform or the quality of capacity development training. Therefore, the ability to autonomously and continuously improve their capacities is not required. Furthermore, as the questions are not prioritised, the GCI has been assessed as not being suitable for a step-by-step measure of national capacity[127]. Therefore, the GCI is not suitable as a checklist for considering national cybersecurity strategies.

For this reason, the CSCMMN was adopted as the starting point for the creation of the evaluation model in this paper.

The CSCMMN was published in 2014 by The Global Cyber Security Capacity Centre, an organisation led by the University of Oxford, and is currently in its latest edition in 2021. The CSCMMN is designed to help countries systematically and effectively improve their cybersecurity capabilities and has been assessed as having the features needed to improve national cybersecurity strategies[128]. The indicator consists of the following five Dimensions, each of which is categorised into 24 'factors' and further divided into 53 'aspects'. Furthermore, in each Aspect, there are five levels of maturity.

1. Devising cybersecurity policy and strategy
    - D.1.1: National Cybersecurity Strategy
    - D1.2: Incident Report and Crisis Management
    - D1.3: Critical Infrastructure (CI) Protection
    - D1.4: Cybersecurity in Defense and National Security
2. Encouraging responsible cybersecurity culture within society

D2.1: Cybersecurity Mindset

D2.2: Trust and Confidence in Online Service

D2.3: User Understanding of Personal Information Protection Online

D2.4: Reporting Mechanisms

D2.5 Media and Social Media

3. Developing cybersecurity knowledge

D3.1: Building Cybersecurity Awareness

D3.2: Cybersecurity Education

D3.3: Cybersecurity Professional Training

D3.4: Cybersecurity Research and Innovation

4. Creating effective legal and regulatory frameworks

D4.1: Legal and Regulatory Provisions

D4.2: Related Legislative Framework

D4.3: Legal and Regulatory capability and Capacity

D4.4: Formal and Informal Co-operation Frameworks to Combat Cybercrime

5. Controlling risks through standards, organizations andtechnologies

D.5.1: Adherence to Standards

D5.2: Security Controls

D5.3: Software Quality

D5.4: Communications and Internet Infrastructure Resilience

D5.5: Cybersecurity Marketplace

D5.6: Responsible Disclosure

This classification of CSCMMN was developed as an evaluation model for Disinformation based on the following ideas, also taking into account the Disinformation measures of the countries that have

been investigated so far.

First, as Disinformation has the nature of both a cyberspace problem and a security issue, it is necessary to evaluate both aspects. In light of this, for D1, the National Defence Strategy section, which had been a Factor in D1-4, was elevated to a Dimension, and the two sections "Cybersecurity Policy and Strategy" and "Defence Strategy" were added to D1. Defence Strategy".

As D2 and D5 are rather broad categories to be applied to Disinformation, they were combined into one category as D6, a new model for comprehensive measures such as collaboration with platforms.

D3 is organised as measures for fact-checking and literacy education by applying it to Disinformation.

D4 is set as D3 in the new model as a category of laws and regulations of Disinformation. However, in Disinformation, laws and regulations to protect election security are even more important because major manipulations have been carried out in elections in various countries, as can be seen from the state of countermeasures in various countries. Therefore, among the legal and regulatory frameworks, those related to election security were set as a separate Dimension and made a priority assessment item.

The number of factors in the Dimension was unified into the top five priority items to ensure a fair balance between the Dimensions, and while the selection method of the five items conforms to the CSCMMN to some extent, it also reflects the countermeasure situation in each country, so it cannot escape criticism that this point is subjective. Criticism that the selection of the five items is subjective in this respect is inescapable. Further discussion is needed on this point.

In terms of the level of countermeasures, the CSCMMN has a set of five levels, but it should be noted that countermeasures against disinformation in cyberspace are relatively new initiatives that have progressed rapidly over the past five to six years, and that disinformation is a more specific and narrower concept than cybersecurity. As it is a more specific and narrow concept, it was considered difficult to set the same level of awareness as the CSCMMN. Therefore, it was decided to organise and score the measures in three levels: 'whether such measures are actually being taken' (=2 points), 'not implemented but under consideration by Parliament or others, or there are similar policies' (=1 point), and 'no such measures are being taken at all' (=0 points).

The evaluation model for Disinformation measures developed from the above perspective is shown in Table 5.

For D 1, factors such as 'disinformation countermeasures are incorporated into the cyber security strategy' and 'the competent authorities and corresponding units for disinformation countermeasures are defined and the necessary budget is allocated' were included based on the need to strategically deal with information warfare, including disinformation, as a state. The elements were included. The CSCMMN also incorporates critical infrastructure as a Factor and, as Disinformation operations are an attack on the values and institutions of democracy, it mentions that 'CI designation of elections

infrastructure as a countermeasure against Disinformation'. In addition, data collection for attribution is essential in implementing Disinformation measures, and at the same time, from the perspective of whether the issue of conflicting legal interests, such as the secrecy of communications, can be cleared, the Factor that "the government can intercept communications and collect bulk data as a Disinformation measure is The Factor that "the administration can intercept communications and collect bulk data as a disinfo measure" is set. And in order to fight back against such operations as a state, the Factor is also that "policy ACD, such as financial sanctions, prosecution and diplomatic name-calling and criticism, can be carried out against the Disinfo Op".

As the discussion so far has confirmed, Disinformation operations are handled by the military and intelligence departments on the attacker's side, with Disinformation being a security issue. Therefore, as the defence side needs to deal with the same level of operations, D2 has set the following Factor. 'National defence departments have mechanisms in place to deal with disinformation' and 'have the intelligence community embedded in their countermeasures', which is necessary in light of the attacker's system. And since these operations also target our cognition, they must "have an all-domain military strategy that includes the cognitive domain". In addition, the ability to fight back more aggressively than policy-based ACD is an evaluation point for countermeasures, so it is necessary to be able to "conduct ACD against disinfo Op for attribution resolution, such as intrusion or hackback against the other party" and to "conduct ACD against disinfo Op for takedown of the other party's site or domain, communication blocking and malicious attacks against the other party's site or domain". The Factor incorporates that "technical ACD can be carried out against the disinfo Op, such as takedown of the other party's site or domain, blocking communications or counterattacking through the use of malware".

D3 incorporates various types of legislation as a factor: as Disinformation operations are conducted by foreign powers in a manner similar to interference in internal affairs, the Factor states that "legislation is in place to investigate and punish foreign interference", and that Disinformation is a so-called Factor is that "there is legislation to control the dissemination of false information", given the nature of false information, such as so-called fake news. On the other hand, the determination of what is false and what is Disinformation must not be arbitrary, and as long as laws and regulations are made as an act of the State, it is necessary that the decentralisation of judicial, legislative and administrative power is established ('decentralisation is established for the recognition of falsehoods and disinformation'). And, as laws and regulations centred on social networking sites, the first requirement is to clarify the senders of disinformation, so "there are schemes to encourage platforms to respond to the transmission of information suspected of disinformation, including the disclosure of sender information and the deletion of information" and "for the distribution of political advertisements Factors such as 'There is legislation to increase transparency in the distribution of political advertisements' were set.

Based on past cases, D4 focuses on preventing interference by foreign powers in elections and the dissemination of false information, enabling attribution to the originators of disinformation, and preventing coordination with information-stealing cyber-attacks. In these terms, the following are some of the key issues that need to be addressed: legislation is in place to investigate and punish foreign interference in democratic processes such as elections; legislation is in place to control the dissemination of false information for the purpose of harming the fairness of elections; legislation restricts campaigning by foreign nationals; and during elections, legislation is in place to prevent the disinformation of candidates and parties from being targeted. Factors such as: there is a scheme for prompt disclosure and suspension of disinformation to candidates and political parties during elections; and there is a mechanism to provide cybersecurity support to political parties and candidates to prevent hacking that could serve as a basis for disinformation operations.

In D5, the cybersecurity knowledge and education aspects of D3 of the CSCMMN were applied to disinformation measures, with Factors on fact-checking measures and improving literacy. In policy-related content, it is not possible to gain trust if the information is only communicated from the government's perspective, so it is important for both the public and private sectors to work together from multiple angles. For this reason, two factors were set: the existence of public fact-checking transmissions and the existence of private sector fact-checking organisations active in the field. Furthermore, as mentioned above, due to the importance of measures in elections, the element 'there is an election-specific fact-checking dissemination' was also set. And in terms of literacy, because measures for people other than young people who can be educated are also needed, and because it is necessary to provide not only simple media literacy education, but also guidance based on the characteristics of disinfo, the elements "media literacy with a focus on disinfo, targeting all voters, with efforts are being made" and that "education with disinfo in mind is being introduced into public education, including the cultivation of critical thinking, the RAVEN method, the study of logical fallacies and the dissemination of knowledge on methods of attack on the cognitive domain" as factors.

D6 elements comprehensive measures that cannot be classified under the previous Dimensions. It incorporates the perspectives of international cooperation, public-private collaboration, technical measures and human resources development, and includes the following elements: participation in international norms on disinfo, such as the Paris Call; a framework for governments and platforms to work together on disinformation measures; a framework for platforms to have regulatory authority over ad networks and algorithms. The following elements were set: 'Has regulatory authority over ad networks and algorithms', 'Has initiatives to provide countermeasure functions such as automatic detection, notification and reporting in SNS and messenger apps', and 'Has a system to train and support researchers in SNS analysis and deepfake research as a countermeasure against disinformation'. The following elements were set out.

Then, as target countries for comparison with Japan, this paper selected the USA, the UK, Germany,

France, Singapore and Taiwan. The four Western countries were chosen because they have experienced election interference allegedly by Russia and have been among the first countries to formulate disinformation measures. Singapore was also selected because it is located in Asia, the same region as Japan, and because it is unique in that it has developed strong legal measures with somewhat authoritarian characteristics, as described in Chapter 6, and has adopted a stance of eliminating interference by foreign powers. Taiwan was selected because it is located in Asia, like Japan, and has actively developed a number of disinformation measures after experiencing repeated election interference and disinformation cyber-attacks from China.

Chart.1 shows the results of the evaluation of each country in Table 5. The chart clearly shows that Japan is very far behind in disinformation countermeasures compared to the countermeasures taken in other countries.

The Evaluation Model for Nations against Disinformation							
(Yes＝2points, TBD=1point, No=0point. TBD means "partially implemented" or "under consideration".)							
Dimension 1: Cybersecurity Policy and Strategy							
Factor	**US**	**UK**	**Germany**	**France**	**Singapore**	**Taiwan**	**Japan**
D 1.1: The cybersecurity strategy integrates concepts of tackling Disinfo.	2	1	2	2	0	2	1
D 1.2: The competent authorities for tackling disinfo are defined and the necessary budget is provided for it.	2	2	2	2	1	2	1
D 1.3: Election infrastructure is designated as the critical infrastructure for disinfo countermeasures.	2	1	1	1	0	0	0
D 1.4:Administrative agencies can intercept communications and collect bulk data for disinfo countermeasures.	2	2	1	1	2	2	0
D 1.5: Policy ACD, including financial sanctions, prosecution and name and shame, can be operated against disinfo Op.	2	2	0	1	2	2	1
	10	8	6	7	5	8	3
Dimension 2 : Defence Strategy							
Factor	**US**	**UK**	**Germany**	**France**	**Singapore**	**Taiwan**	**Japan**
D 2.1: National defence agencies have some functions to tackle disinfo.	2	1	1	1	0	2	1
D 2.2: Intelligence communities are integrated into disinfo measures.	2	2	2	2	1	2	0
D 2.3: All-domain military strategy has been developed, including in the cognitive domain.	2	1	1	1	0	2	2
D 2.4: ACD for attributional resolution, such as intrusion or hack-back to the adversary, can be operated against disinfo Op.	2	1	1	2	0	1	0
D 2.5:Technical ACD, including takedown of adversarys' websites and domains, communication blocking and counter-attacks using malware can be operated against disinfo Op.	2	2	1	2	0	1	0
	10	7	6	8	1	8	3
Dimension 3: Legal and Regulatory Frameworks							
Factor	**US**	**UK**	**Germany**	**France**	**Singapore**	**Taiwan**	**Japan**
D 3.1: Legislation is in place to investigate and punish foreign interference.	2	1	0	1	2	2	0
D 3.2: Legislation is in place to regulate the dissemination of false information.	2	2	2	2	2	2	2
D 3.3 Separation of powers is in force with respect to the judgement of false information or disinformation.	2	2	2	2	0	2	2
D 3.4:Legal schemes are in place to encourage platforms to respond to suspected disinformation by disclosing sender information, deleting information, etc.	1	1	2	2	2	2	0
D 3.5: Legislation is in place to increase transparency regarding the algorithms and funding relationships for political advertising distribution on websites and social networking sites.	1	1	2	2	0	1	2
	8	7	8	9	6	9	6

Dimension 4: Election Security							
Factor	**US**	**UK**	**Germany**	**France**	**Singapore**	**Taiwan**	**Japan**
D 4.1: Legislation is in place to investigate and punish foreign interference in elections and other democratic processes.	2	1	1	1	2	2	0
D 4.2: Laws are in place to regulate the dissemination of false information for the purpose of harming the fairness of elections.	2	1	2	2	2	2	2
D 4.3: Electoral campaigning by foreign nationals is restricted to a certain extent.	1	1	1	1	1	1	0
D 4.4: During elections, there is a legal scheme that allows for sender disclosure and suspension of disinformation targeted at candidates and political parties.	1	1	2	2	1	2	0
D 4.5:Programs exist to provide cybersecurity assistance to political parties and candidates to prevent hacking that would constitute information theft used for disinfo operations.	2	2	1	2	0	1	0
	8	6	7	8	6	8	2
Dimension 5: Fact check and Media Literacy							
Factor	**US**	**UK**	**Germany**	**France**	**Singapore**	**Taiwan**	**Japan**
D 5.1: The government is taking the initiative in disseminating public fact-checking.	2	0	2	0	2	2	0
D 5.2: Private fact-checking organizations affiliated with The International Fact-Checking Network (IFCN) are active.	2	2	2	2	0	2	2
D 5.3:Fact-checking dissemination is provided specifically for elections by public and private sectors.	2	1	2	1	1	2	1
D 5.4:The state is providing media literacy education for all voters with a focus on disinfo.	2	1	1	1	1	2	0
D 5.5:Education, including countermeasures against disinfo such as the cultivation of critical thinking, the RAVEN method, the learning of logical fallacies, and of the knowledge about attacks on the cognitive domain, are introduced into public education.	2	1	1	1	1	2	0
	10	5	8	5	5	10	3
Dimension 6: Comprehensive countermeasures							
Factor	**US**	**UK**	**Germany**	**France**	**Singapore**	**Taiwan**	**Japan**
D 6.1: The government participates in international norms related to disinfo, such as the Paris Call.	2	2	2	2	0	0	2
D 6.2: A framework has been developed for the government and platforms to work together to combat disinformation.	1	1	1	1	1	2	0
D 6.3: The government has regulatory authority over ad networks and algorithms for platformers.	1	2	1	1	0	1	0
D 6.4: Efforts are being promoted to add countermeasure functions to SNS and messenger apps, such as automatic detection, notification, and reporting of disinformation.	2	1	1	1	0	2	0
D 6.5: As a disinfo countermeasure, the government is training and supporting researchers in social network analysis, deep-fake research, and other areas.	2	1	0	0	0	1	1
	8	7	5	5	1	6	3

Table 5 The Evaluation Model for Nations against Disinformation

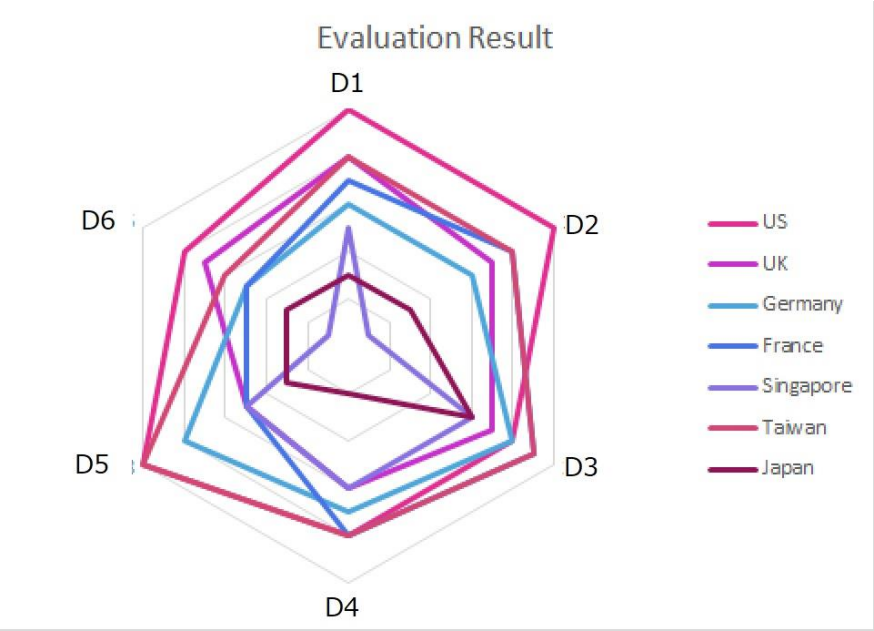

Chart 1 the result of the evaluation model

7-2. National Security Challenges of Japan

This section summarises the challenges of disinformation countermeasures in Japan from the scoring in this evaluation model.

First, from the perspective of national strategy, the concepts of information warfare and cognitive warfare were incorporated for the first time in the new National Security Strategy[129] approved by the Cabinet in December 2022. The description in this strategy marks the stage at which the development of the system will finally begin. Compared with other countries that have already made various efforts, it is undeniable that the Japanese Government needs to make efforts to make up for this delay. Furthermore, as discussed in the previous chapters, disinformation operations in recent years have mainly been conducted in cyberspace, so it will be necessary to incorporate disinformation countermeasures into cybersecurity strategies in the future. And to ensure that such a strategy does not turn out to be a pipe dream, the conflict with the secrecy of communications in the Constitution must be resolved so that data interception by the public administration is possible. Furthermore, it is also necessary to develop a system that allows for judicial prosecution and financial sanctions as part of policy ACD when attacks by state actors are discovered.

From the perspective of defence strategy, the establishment of a specialised intelligence unit in the Ground SDF to deal with cognitive warfare, along with the revision of the National Security Strategy, is a step forward. However, influence operations, including disinformation, and countering them are conducted by many countries with the participation of intelligence agencies, and it must be said that Japan, without a foreign counter-intelligence agency, is in a lopsided situation. Previous studies have

already pointed out that in many countries, intelligence agencies play a central role in cybersecurity[130], and that a factor is that the attribution response, which anticipates and prevents cyber-attacks in advance and identifies potential attackers, is similar to espionage and is the extension of this process. This argument can also be applied to disinformation countermeasures, as there are many cases where disinformation dissemination and cyber-attacks are combined in influence operations, and attribution of the source of disinformation operations alone is also crucial. Therefore, in order to fight the information and cognitive warfare in Japan, it will be necessary to develop sufficient intelligence agencies in the future. In addition, surveillance and cyber counter-attacks will require partial amendments to relevant laws, such as the Constitutional Secrets of Communications and the Unauthorised Computer Access Law, which are barriers to such counter-attacks.

In terms of countermeasures through the legal system, including elections, the Criminal Code provides for the offences of dissemination of false information and defamation, and the Public Offices Election Law provides for the offence of publishing false matters (Article 235(2)), so among disinformation, there are certain checks on so-called fake news and hate speech. This is a certain measure to prevent so-called fake news and hate speech from being used among disinformation. On the other hand, the legal system is not well developed in terms of preventing foreign powers from interfering in internal affairs. There is no legal system to investigate and punish interference by foreign powers, either in peacetime in general or during elections, and there are no certain restrictions on the political campaigning of foreigners in elections. Although it is difficult to obtain a legal basis from current domestic laws to prohibit foreign election campaigning or directly prohibit electioneering by foreign governments, it should be considered that international law has the principle of non-interference in domestic affairs, which can limit the influence of foreign governments and election campaigning. The Guidelines for the Revised Public Offices Election Law[131] clearly state that "foreigners are not prohibited from election campaigning under the current law, and may continue to do so even after the ban on internet election campaigning is lifted", but the involvement of foreign governments with the intention of interfering in Japanese politics should naturally be prevented. This should be the case. In this age of disinformation, the approach of these guidelines is also required to change in line with the trends of the times.

With regard to the dissemination of fact-checking, the Japan Fact-check Center (JFC) was established in October 2022, becoming the first private fact-checking organisation in Japan to join The International Fact-Checking Network (IFCN). However, there has been no public fact-checking or counter-narrative dissemination by the government itself, and it will be necessary for both the public and private sectors to work together in the future. It is also necessary to incorporate media literacy education for voters and youth into public education, while also working with media and platforms.

With regard to comprehensive measures, the challenge is to actively promote initiatives in collaboration with platform operators, as in the EU. The final report of the study group on platform

services led by the Ministry of Internal Affairs and Communications, published in February 2020,[132] concluded that "it is appropriate to promote measures based on voluntary initiatives by the relevant parties in the private sector, including platform operators". Of course, from the perspective of freedom of expression, it is not permissible for the government to impose regulations such as censorship, but we believe that encouraging operators to take initiatives to improve transparency and requiring regular reporting, as in the EU Code of Conduct, is a range that can be adequately addressed within the current constitutional framework. It is obvious from the case studies conducted so far that the EU and national governments are taking measures because there are limits to what can be achieved through voluntary initiatives, and Japan will be forced to take similar measures sooner or later.

Finally, a discussion is presented on the concerns underlying various countermeasures against disinformation, such as removing disinformation on the web, government fact-checking and platform regulation, that these measures may correspond to government censorship and infringe freedom of expression. For this, reference is made to the case of Judgment upon case of constitutionality on customs inspection (12.12.1984, 1982 (Gyo-Tsu) 156, Minshu Vol. 38, No. 12 at 1308). First, it is said that the prohibition against censorship in the first sentence of Article 21(2) of the Constitution should be interpreted as not permitting exceptions on the grounds of public welfare. The term 'censorship' as used in Article 21(2) of the Constitution refers to 'censorship of the content of ideas and other forms of expression by the administrative power as the subject matter, with the aim of prohibiting the publication of all or part of the content of ideas and other forms of expression, by examining the content of certain forms of expression to be covered, in a comprehensive and general way, before publication and prohibiting the publication of those that are deemed inappropriate'. The court held that the term "censorship" should be interpreted as having as its characteristic feature the prohibition of the publication of material that is found to be unsuitable. According to this definition of censorship, restricting the dissemination of web media articles and social networking posts that are subsequently found to be disinformation by a foreign power after an investigation of the sender and the facts does not constitute censorship. In addition, if the sender is a foreign web media outlet, such as RT, and disinformation directed at Japan is only restricted by deleting the account, it does not constitute censorship, as the opportunity to publish is also available outside Japan and is not entirely taken away[133]. Furthermore, the case law states that when it is permissible to give a limited interpretation to a provision of a law regulating freedom of expression, "the interpretation must clearly distinguish between what is subject to regulation and what is not, and must make clear that only what can be constitutionally regulated is subject to regulation" and that "the interpretation must be based on the fact that the law is not a censorship law". The provisions must also be read in such a way that the general public can understand the criteria that enable them to determine whether or not the expressive material is subject to regulation in a specific case". As for the various regulations on measures against disinformation, the regulations should focus on disinformation from foreign powers as a matter of

security, and in a liberal democratic state, the transmission of misinformation by its own citizens must be tolerated to some extent in the free marketplace of ideas. From this perspective, if the regulation is limited to disinformation by foreign powers, the target of the regulation is clear and generally understandable. Chapter 6 also touched on the problems of authoritarian state regulation, but Japan, as a liberal democratic state, should take an autonomous stance in resolving issues.

As mentioned above, there are many challenges for Japan, which is lagging behind in disinformation measures. Based on the above, the next chapter will examine policy recommendations for Japan in relation to disinformation measures, and will also refer to what each country should aim for as a standard.

8. Conclusion

8-1. Policy Recommendation for Japan

Based on the above policy assessment, the following disinformation measures are recommended for Japan[134].

1. Establishment of monitoring centre to combat disinformation

(1) In order to combat disinformation by foreign actor aiming the democratic electoral process, an monitoring centre collecting information on interference by foreign powers using disinformation shall be established.

At the centre, monitoring, research and analysis of activities similar to foreign disinformation shall be carried out. It will also be responsible, together with the judicial authorities, for operations in response to foreign disinformation. The Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Disclosure of Identification Information of Senders (Provider Liability Limitation Act) will be amended to enable these activities to be carried out effectively. Additionally, in future, Japan needs to establish the strong counter-intelligence agency to combat disinformation, influence operations and finally information warfare as the previous chapter pointed out. This monitoring center is just the starting point, and it should be positively dissolved and absorbed into new intelligence agency.

(2) Consider enacting a law that enables the imposition of ex post sanctions and countermeasures permitted under international law against disinformation attacks.

The Public Offices Election Law and the Law on Procedures for Amending the Constitution of Japan (Referendum Law) should be amended to crack down on interference by foreign powers using disinformation. In doing so, the right to knowledge of the people guaranteed by the Constitution of Japan should be taken into account. In doing so, the State should actively disclose information on the crackdown, paying attention to the right to knowledge of the people guaranteed by the Constitution of Japan.

2. Designation of electoral infrastructure as critical infrastructure

(1) Actions will be taken based on severity assessments in line with the designation as critical infrastructure.

(2) Establish an Information Sharing and Analysis Centre (ISAC) and make incident reporting and sharing mandatory.

(3) During elections, the Government will provide cyber security support to political parties and electoral commissions.

(4) Appropriate cybersecurity support should also be provided to polling systems that influence election results.

Designate electoral infrastructure as critical infrastructure and make it a priority cybersecurity protection target. Create an Election Management ISAC with local government electoral commissions as constituents to share and collaborate on cyber threat information and implement effective security policies or guidelines.

Specifically, the 14 sectors currently identified as 'critical infrastructure sectors' - 'information and communications', 'finance', 'aviation', 'airports', 'railways', 'electricity', 'gas', 'government and administrative services (including local authorities)', 'healthcare', 'water', 'logistics', 'chemicals', 'credit' and 'petroleum' - will be included in the ISAC. Of the 'Election system', 'Election system' is set under the 'Government and administrative services (including local authorities)' sector. It defines 'casting and counting systems', 'electronic voting systems', 'tabulation systems' and 'information dissemination media for each electoral authority' as its protective objects.

3. Active Cyber Defence (ACD) system

(1) Attribute disinformation operating entities.

(2) Establish legislation to conduct ACD as a legitimate business act of the State even in peacetime.

(3) Adequate budgetary measures should be taken to ensure effective attribution through cooperation between the public and private sectors.

To counter foreign disinformation, apart from judicial ex post sanctions and crackdowns to conduct ACD, including conducting attribution on the attacking entities. In addition, legislation such as the concept of secrecy of communications in the Constitution or Act on Prohibition of Unauthorized Computer Access should be amended and developed so that ACD can be carried out as a legitimate business act of the State. In these efforts, Japan, together with our allies, declares that we will take all possible measures, including strategic communication, to counter disinformation.

4. Cooperative regulatory efforts by the government and platformers and formulation of a code of conduct

(1) With reference to precedents in the EU and the UK, consider a system of cooperative regulation of disinformation by the government and platformers, while taking into account restrictions on freedom of expression and confidentiality of communications in Japan, and respecting voluntary efforts by platformers.

(2) Develop a code of conduct for platformers in Japan, setting out the direction for cooperative regulatory efforts. This code of conduct should include the following items; ① Establishment of a system for reporting and removing false information; ② Establishment of a system for reporting and removing bot accounts; ③ Ensuring transparency regarding diffusion algorithms; ④ Ensuring transparency regarding political advertising; and ⑤ Requiring platforms to post links to original articles when reproducing news from existing news organisations.

(3) Designate SNS operators as 'specified digital platform providers' in the Law on Enhancing Transparency and Fairness of Specified Digital Platforms (Digital Platform Transparency Law) as regulated operators, and require them to comply with Article 5 'Terms and Conditions of Provision of Specified Digital Platforms'. Disclosure of Terms and Conditions of Provision of Specific Digital Platforms", and promote transparency in the distribution of political advertisements.

5. Enhance the media literacy education and fact-checking

(1) With disinformation in mind, introduce programmes to enhance media literacy into primary and secondary education in a manner that is clearly stated in the Courses of Study. (2) Work on the cultivation of critical thinking, the RAVEN method, the study of logical fallacies, and the dissemination of knowledge on methods of attack on the cognitive domain.

(2) Leaflets on media literacy during elections are prepared and distributed together with election publicity.

(3) Establish a government fact-checking portal. The Government will not disseminate information on the content, but will only operate the portal and establish a mechanism for the public to know what kind of disinformation is currently being talked about and disseminated. Fact-checking will be outsourced to private organisations, and a fact-checking platform will be set up with the participation of major media, universities and think tanks. The portal will be equipped with a mechanism for registering organisations, so that the fact-checking of various organisations can be compared and viewed. In addition, a White Paper on Disinformation will be published by the Government.

(4) Adequate budgetary measures, such as the use of universal service charges, should be taken to cover the costs of fact-checking.

(5) Establish a fact-checking system during election periods. In the US, a presidential decree was issued in 2018 ordering intelligence agencies to investigate the existence of foreign interference in elections within 45 days of a national election. As in the US, the Government will take the lead in checking whether falsehoods in breach of the Public Offices Election Law are disseminated during the election period. For this purpose, fact-checking bodies will be accredited at the time of the election.

8-2. Strategic Goals against Disinformation

Following the policy recommendation for Japan, the strategic goals against disinformation for each nation are posed in this section as the conclusion.

As for individual national strategies, it is important to fulfill the factors of each dimension listed in the evaluation model in a balanced approach. Since this model is created for liberal democratic nations taking countermeasures against disinformation, the separation of powers and protection of fundamental human rights must be firmly maintained in every situation of data collection and investigation, punishment of attackers by the state power. Furthermore, as some research[135] referred,

the disinformation tactics must be never applied as the democracies' countermove against the disinformation of adversaries, because they compromise the value of democracy. These are the challenges that each country should strategically address with dignity and autonomy as a liberal democratic nation.

In terms of the next goal at the regional level, similar to EU, the Indo-Pacific region should cooperate to counter China's intelligentized warfare based on changing the status quo by force. To this purpose, an initiative of "the Free and Open Indo-Pacific Strategy (FOIP) vs. Disinfo" is proposed here, modeled after EU vs Disinfo. Tackling disinformation is suitable to the core idea of the FOIP concept which is to establish a rules-based international order and consolidate principles such as free trade, freedom of navigation, and the rule of law, which are essential for the stability and prosperity of the region. In order to enhance security in the region against the disinformation and strategic narratives that China operates in this region, a system of cooperation and deterrence through information and technology sharing across countries is necessary. Furthermore, this region should naturally cooperate with European nations as well, as China and Russia's information warfare is conducted throughout the world.

A proposal for an Indo-Pacific hybrid threat center by Australian Strategic Policy Institute[136] is instructive in establishing this structure. Since disinformation is a part of hybrid threats, it would be effective that such a center leads the initiative titled FOIP vs Disinfo to study cases in the Indo-Pacific region, formulate common disinformation countermeasures, provide support to countries for devising countermeasures, and disseminate information such as fact checking. However, since the FOIP strategy was proposed by Japanese Prime Minister Abe in 2016[137], Japan is expected to be actively involved and take the lead in this initiative.

While the discussion in Chapter 5 indicates that international legal restrictions on disinformation are difficult to enforce, at the normative level, it is desirable to formulate new norms that would restrain state involvement in disinformation operations. This point has not been fully explored in this thesis and is an issue for future work.

This paper presents the evaluation model for nations against disinformation to contribute to the survival of liberal democracies in the age of disinformation, in accordance with law, order and democratic value. However, in the information warfare waged in the cyber and cognitive domains, both attackers' and defenders' technologies are advancing at a dizzying pace, and this model may need to be revised in line with the changing situation.

May this research serve as a contribution to the security of Japan and other countries that advocate liberal democracy.

Acknowledgement

Firstly, I would like to express my sincere gratitude to my supervisor Prof. H. Yuasa for the continuous support from my master to my Ph.D. study and related research, for his patience, motivation and kind advice based on insightful immense knowledge, even after he moved from IISEC to Meiji University. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my research period.

Additionally, I would like to thank my present supervisor Prof. H. Doi for the support of a lot of procedure to submit the thesis and related matters.

Besides my advisors, I would like to thank the rest of my thesis committee: Prof. T. Okubo and Prof. Y. Murakami for their instructive comments and encouragement, and also for the challenging questions which leads me to widen my research from various perspectives.

I thank the member of Yuasa Lab. who provides me a lot of diversified and inspiring comments to my research in the seminar, and thank all professors and staff of the Institute of Information Security for their guidance and great support.

Furthermore, I would like to express my gratitude to the team of the cybersecurity program in the Sasakawa Peace Foundation, especially a senior researcher Mr. Osawa. The experience of writing the policy recommendation regarding disinformation under his leadership and guidance provided me the great opportunity to deepen my research of this thesis.

At last, I would like to thank my friends and my family for supporting me spiritually throughout writing this thesis and my life in general.

[1] T. Rid, 2020, *Active Measures: The Secret History of Disinformation and Political Warfare*, New York: Farrar, Straus and Giroux.
[2] Ibid.
[3] JOURNAL OF INFORMATION WARFARE (https://www.jinfowar.com/)
[4] From the perspective of the right to know in a free marketplace of ideas, some have questioned the regulation of disinforamtion from abroad and that within one's own country by distinguishing between sources of disinforamtion. (e.g., Erwin Chemerinsky, 2018, *Fake News and Weaponized Defamation and the First Amendment*, 47 Sw. L. Rev. 291-296., Eijiro Mizutani, 2019, "Fake News" in the free marketplace of idea, Keio media communications research, vol.69, 55-68.) However, as this paper discusses the issue of disinformation from the perspective of national security and strategy, it does not elaborate on the issue of freedom of expression in the Constitution.
[5] P. Brangetto and M. A. Veenendaal, Influence Cyber Operations: The use of cyberattacks in support of Influence Operations, p115, 2016 8th International Conference on Cyber Conflict (CyCon), 2016, pp.113-126.
[6] US Department of Defense, Directive 3600.01. May 2, 2013. p.12.
[7] Sean Cordey, 2019, Cyber Influence Operations: An Overview and Comparative Analysis, Center for Security Studies (CSS).
[8] EUvsDisinfo (https://euvsdisinfo.eu/)
EUvsDisinfo is the flagship project of the European External Action Service's East StratCom Task Force(opens in a new tab). It was established in 2015 to better forecast, address, and respond to the Russian Federation's ongoing disinformation campaigns affecting the European Union, its Member States, and countries in the shared neighbourhood.
[9] The Kremlin, "Address by the President of the Russian Federation," 24 February 2022. (http://en.kremlin.ru/events/president/news/67843)
[10] Reuters, "US, UK: Russia responsible for cyberattack against Ukrainian banks," 19 February 2022. (https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/)
[11] Bloomberg, "Russia's Cyberwar on Ukraine Aims to Damage Psyche Not Pocketbook," 23 February 2022. (https://www.bloomberg.com/news/newsletters/2022-02-23/russia-s-cyberwar-on-ukraine-aims-to-damage-psyche-not-pocketbook)
[12] Ministry of Defence of the Russian Federation, "Statement of the Russian Defence Ministry spokesperson, Major General Igor Konashenkov, on the return of formations and military units to permanent locations," 15 February 2022. (https://eng.mil.ru/en/news_page/country/more.htm?id=12408929@egNews)
[13] The White House, Remarks by President Biden Providing an Update on Russia and Ukraine, 18 February 2022. (https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/18/remarks-by-president-biden-providing-an-update-on-russia-and-ukraine-2/)
[14] Two typical examples are as follows.
Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare, 2020.
Claire Wardle, PhD and Hossein Derakhshan (2017) Information Disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe.
[15] Claire Wardle, PhD and Hossein Derakhshan (2017) Information Disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe. p5.
[16] the independent High level Group on fake news and online disinformation (2018) A multi-dimensional approach to disinformation. European Commission. p5.
[17] 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).
[18] "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)

[19] "France election: Macron laughs off gay affair rumours" https://www.bbc.com/news/world-europe-38892409

[20] See also note 4 as for the disclaimer regarding the conflict with the freedom of speech.

[21] Marc Laity, 2015, NATO AND THE POWER OF NARRATIVE, Peter Pomerantsev ed., *Information at War: From China's Three Warfares to NATO's Narratives*, London: LEGATUM INSTITUTE, 22-27.

[22] *Ibid.*

[23] Sternberg, R. J., & Sternberg, K., 2017, *Cognitive psychology (7th edition)*, Wadsworth: Cengage Learning.

[24] C4ISRNET, "DIA director: We are preparing to fight the last war," 15 August 2017. (https://www.c4isrnet.com/show-reporter/dodiis/2017/08/14/dia-director-we-are-preparing-to-fight-the-last-war/)

[25] U.S. Air Force, "Air Force Association 2017 Air, Space & Cyber Symposium Remarks by General David L. Goldfein U.S. Air Force Chief of Staff," 19 September 2017. (https://www.af.mil/Portals/1/documents/csaf/CSAF_AFA_2017%20Air_Space_and_Cyber_Symposium.pdf)

[26] INNOVATION HUB, "Cognitive Warfare Project- Reference Documents" (https://www.innovationhub-act.org/cw-documents-0)

[27] F. Cluzel, 2020, "Cognitive Warfare," INNOVATION HUB. (https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf)

[28] R. Alderman, "Domains of warfare and strategic offsets," Military Embedded systems, 31 January 2017. (https://militaryembedded.com/comms/satellites/domains-of-warfare-and-strategic-offsets)

[29] Y. Rosner and D. Siman-Tov, "Presidential Elections: The New Threat of Cognitive Subversion," INSS Insight No. 1031, 8 March 2018. (https://www.inss.org.il/publication/russian-intervention-in-the-us-presidential-elections-the-new-threat-of-cognitive-subversion/)

[30] D. Mackiewicz, 2018, "Cognitive Warfare: Hamas & Hezbollah and their insidious efforts," Tel Aviv: INSS-Summer Institute. (https://www.researchgate.net/publication/337228818_Cognitive_Warfare_-_Mackiewicz-Diana_2018)

[31] P. Ottewell, "Defining the Cognitive Domain," OTH, 7 December 2020. (https://overthehorizonmdos.wpcomstaging.com/2020/12/07/defining-the-cognitive-domain/)

[32] L. K. Bjørgul, "Cognitive warfare and the use of force," Stratagem, 3 November 2021. (https://www.stratagem.no/cognitive-warfare-and-the-use-of-force/)

[33] Carl von Clausewitz, 1832, Vom Kriege, Berlin: Ferdinand Dummler. (Michael Howard and Peter Paret, trans., 1993, ON WAR, London: Everyman's Library.)

[34] The Soufan Center, "QUANTIFYING THE Q CONSPIRACY: A Data-Driven Approach to Understanding the Threat Posed by QAnon," 2021.

[35] Office of the Director of National Intelligence, "Domestic Violent Extremism Poses Heightened Threat in 2021." March 17, 2021. (https://www.dhs.gov/publication/domestic-violent-extremism-poses-heightened-threat-2021)

[36] Winter, Jana. "Exclusive: FBI Document Warns Conspiracy Theories Are a New Domestic Terrorism Threat." Yahoo! News, August 1, 2019. (https://news.yahoo.com/fbi-documents-conspiracy-theoriesterrorism-160000507.html)

[37] Der Generalbundesanwalt beim Bundesgerichtshof, "Festnahmen von 25 mutmaßlichen Mitgliedern und Unterstützern einer terroristischen Vereinigung sowie Durchsuchungsmaßnahmen in elf Bundesländern bei insgesamt 52 Beschuldigten," 7 December 2022. (https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/aktuelle/Pressemitteilung-vom-07-12-2022.html?nn=478184)

[38] Diaz Ruiz C, Nilsson T. EXPRESS: Disinformation and Echo Chambers: How Disinformation Circulates in Social Media Through Identity-Driven Controversies. Journal of Public Policy & Marketing. July 2022. doi:10.1177/07439156221103852.

[39] Joseph E. Uscinski, "Conspiracy Theories: A Primer," 2020, London: The Rowman and Littlefield Publishing.

[40] F. Toriumi "Who is spreading the word on Twitter that the Ukrainian government is a neo-Nazi regime?" Yahoo News, 3 March 2022. (https://news.yahoo.co.jp/byline/toriumifujio/20220307-00285312)

[41] The Communications Security Establishment (2019) 2019 UPDATE: CYBER THREATS TO CANADA'S DEMOCRATIC PROCESS. The Communications Security Establishment.

[42] *Ibid.*, p16.
[43] *Ibid.*, p15.
[44] *Ibid.*, p17.
[45] National Cybersecurity and Communications Integration Center （NCCIC）, “ GRIZZLY STEPPE – Russian Malicious Cyber Activity,” 29 December 2016 （https://us-cert.cisa.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf）
[46] U.S. Senate Select Committee on Intelligence, Hearing, 1 November 2017 （https://www.intelligence.senate.gov/hearings/open-hearing-social-media-influence-2016-us-elections#）
[47] Intelligence Community Assessment, “Assessing Russian Activities and Intentions in Recent US Elections,” Office of the Director of National Intelligence （ODNI）, 6 January 2017 （https://www.dni.gov/files/documents/ICA_2017_01.pdf）
[48] Ibid. p.ii
[49] Alex Isenstadt, John Bresnahan, “Exclusive: Emails of top NRCC officials stolen in major 2018 hack,” POLITICO, 4 December 2018（https://www.politico.com/story/2018/12/04/exclusive-emails-of-top-nrccofficials-stolen-in-major-2018-hack-1043309）
[50] ODNI, “DNI Coats Statement on the Intelligence Community's Response to Executive Order 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election,” 21 December 2018. （https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2018/item/1933-dni-coatsstatement-on-the-intelligence-community-s-response-to-executive-order-13848-on-imposing-certain-sanctionsin-the-event-of-foreign-interference-in-a-united-states-election）
[51] Ellen Nakashima, “U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms,” The Washington Post, 27 February 2019. （https://www.washingtonpost.com/world/nationalsecurity/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc 9 e-36d 6 -11e 9 -af 5 b-b51b 7 ff322e 9_story.html?noredirect=on）
[52] National Intelligence Council, “Foreign Threats to the 2020 US Federal Elections,” 10 March 2021. （https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf）
[53] House of Commons Digital, Culture, Media and Sport Committee, “Disinformation and ‘fake news’ : Interim Report Fifth Report of Session 2017-19,” House of Commons, February 2019, p.43.ff.
[54] https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/171103-Chair-to-Jack-Dorsey-Twitter.pdf
https://www.parliament.uk/globalassets/documents/commons-committees/culture-media-and-sport/171019-Chair-to-Mark-Zuckerberg-Facebook.pdf
[55] Committee on Foreign Relations United States Senate, “Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security,” 10 January 2018, p. 129.
[56] StopFake, “Fake: Merkel Takes Selfie with Belgian Suicide Bomber,” 27 March 2016 （https://www.stopfake.org/en/fake-merkel-takes-selfie-with-belgian-suicide-bomber-2/）
[57] Thomas Davidson and Julius Lagodny, “Germany's far-right party AfD won the Facebook battle. By a lot,” The Washington Post, 26 September 2017 (https://www.washingtonpost.com/news/monkey-cage/wp/2017/09/26/germanys-far-right-party-afd-won-the-facebook-battle-by-a-lot/)
[58] Mark Scott, “Russian ‘botnet’ promotes far-right messages in German election,” Politico, 24 September 2017（https://www.politico.eu/article/russian-botnet-promotes-far-right-messages-in-german-election/）
[59] Lars Petersen, “Hacker attack on the Federal Election Commissioner’s server, ” Business Insider, 15 Sep 2021(https://www.businessinsider.de/politik/deutschland/hackerangriff-auf-server-des-bundeswahlleiters/)
[60] Tagesschau, “Bundesregierung kritisiert Russland scharf,” 6 September 2021

(https://www.tagesschau.de/ausland/cyberangriffe-russland-gru-ghostwriter-101.html)
[61] DW, “Federal government urges Russia to end cyberattacks,” 6 September 2021 (https://www.dw.com/de/bundesregierung-fordert-von-russland-ende-der-cyberattacken/a-59100108)
[62] Der Bundeswahlleiter, “Erkennen und Bekämpfen von Desinformation” (https://www.bundeswahlleiter.de/bundestagswahlen/2021/fakten-fakenews.html)
[63] Volker Witting, Ian Bateson, “German election: The postal vote and fraud claims,” DW, 25 September 2021 (https://www.dw.com/en/german-election-the-postal-vote-and-fraud-claims/a-58844693)
[64] Committee on Foreign Relations United States Senate, “Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security,” 10 January 2018, p.123.
[65] Committee on Foreign Relations United States Senate, “Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security,” 10 January 2018, p.122.
[66] European Comission, “A Europe that protects: EU reports on progress in fighting disinformation ahead of European Council,” 14 June 2019 (https://ec.europa.eu/commission/presscorner/detail/en/ip_19_2914)
[67] Michael Yip, “Taiwan Presidential Election: A Case Study on Thematic Targeting,” PwC, 17 March 2016 (https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.03.17.Taiwan-election-targetting/taiwant-election-targetting.html.pdf)
[68] Nicholas J. Monaco, Google Jigsaw, “Computational Propaganda in Taiwan- Where Digital Democracy Meets Automated Autocracy,”February 2017, p.22.
[69] Kaori Fukushima「Will China collapse inner Taiwan?」『Nikkei Business』28 Novemver 2018 (https://business.nikkei.com/atcl/opinion/15/218009/112700187/)
[70] Ibid.
[71] Nikkei Shimbun,「Taiwan presidential election: debate over 'Chinese election intervention' at Television debate」29 December 2019. (https://www.nikkei.com/article/DGXMZO53986070Z21C19A2FF8000/)
[72] IP Defense Forum, “CCP intervening in 2020 Taiwan elections, wielding many political influence weapons,” 4 December 2019. (https://ipdefenseforum.com/2019/12/ccp-intervening-in-2020-taiwan-elections-wielding-many-political-influence-weapons/)
[73] United States-China Economic and Security Review Commission, “U.S.-CHINA Relations in 2019: A Year in Review,” Hearing, 4 September 2019 (https://www.uscc.gov/sites/default/files/2019-10/September%204,%202019%20Hearing%20Transcript.pdf)
[74] Meta, “Removing Coordinated Inauthentic Behavior From China,” 19 August 2019. (https://about.fb.com/news/2019/08/removing-cib-china/)
[75] Twitter, “Information operations directed at Hong Kong,” 19 August 2019 （https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong）; Nathaniel Gleicher, “Removing Coordinated Inauthentic Behavior From China, ” Meta, 19 August 2019
[76] Ryukyu Shimpou “US plans to deploy new medium-range ballistic missiles in Okinawa, communicated to Russian side within two years, fearing significant amplification of base burden”, 3 October 2019. (https://ryukyushimpo.jp/news/entry-1000469.html)
[77] Hiroyuki Fujishiro, "The Production Process of Fake News Verification Articles - A Case Study of the Okinawa Times in the 2018 Okinawa Prefectural Governor Election", Journal of Social Informatics, Vol. 8, No. 2, The Society for Social Informatics, 2019, pp. 143-157 (http://www.ssi.or.jp/journal/pdf/Vol8No2_ 10.pdf).
The main subject of the article is the case of the Okinawa Times, but it also discusses the fact-checking trend of the Ryukyu Shimpo.
[78] The Ryukyu Shimpo, 'Disinformation on the governor's election, who? The same person's name on two websites. When we track down the identity... ", 1 Jan 2019 (https://ryukyushimpo.jp/news/entry-856174.html).
[79] Public Security Intelligence Agency, "Raising the undecided theory of 'Ryukyu belonging' and China's efforts to shape public opinion in Okinawa", Domestic and Foreign Affairs Retrospect and Outlook, January 2017, p. 23 (http://www.moj.go.jp/content/001221029.pdf).
The 'undecided theory of Ryukyu's belonging' refers to the argument in the Chinese Communist Party's official newspaper, People's Daily, etc., that 'the US has only handed over administrative authority over

the Ryukyu Islands to Japan, and the belonging of the Ryukyu Islands is undecided'. We (China) have called the Ryukyu Islands 'Okinawa' for a long time, but this name is tantamount to our implicit acknowledgement that Japan has sovereignty over the Ryukyu Islands and should not be used".

[80] Takeshi Aragaki, "Exclusive interview with President Putin's aide, Okinawa's bases are an 'obstacle to Japan-Russia relations', Sergei Glazyev points out the harmful effects of subordination to the US," Ryukyu Shimpo, 7 October 2019. (https://ryukyushimpo.jp/news/entry-1002716.html)

[81] On the official website of the Plenipotentiary Representative of the President of the Far Eastern Federal District of the Russian Federation, it is stated that Yuri Trutnev, Deputy Prime Minister of the Russian Federation and Plenipotentiary Representative of the President of the Far Eastern Federal District, will visit Tokyo and Okinawa in October 2018 to meet representatives of the Japanese Government and business community to discuss future cooperation between Japan and the Far Eastern region. "В рамках рабочей поездки Юрия Трутнева пройдет обсуждение сотрудничества Росссии и Японии на Дальнем Востоке, "Официальный сайт полномочного представителя Президента Росссийской Федерации в Дальневосточном федеральном округе, 26 октября 2018. (http://dfo.gov.ru/trutnev/3157/)

[82] Fact vs. Fiction: Russian Disinformation on Ukraine, JANUARY 20, 2022, US Department of State. (Fact vs. Fiction: Russian Disinformation on Ukraine - United States Department of State)

[83] EU vs Disinfo, Disinfo targeting Ukraine (https://euvsdisinfo.eu/category/ukraine-page/)

[84] Putin says some Russian troops are withdrawing after drills, but skepticism in Ukraine and US remains, February 15, 2022,（Countermeasures must be proportionate to the corresponding damage.）

[85] Remarks by President Biden Providing an Update on Russia and Ukraine, FEBRUARY 18, 2022. (https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/18/remarks-by-president-biden-providing-an-update-on-russia-and-ukraine-2/)

[86] The Cylance Research and Intelligence Team, “The Cylance Research and Intelligence Team Reaver: Mapping Connections Between Disparate Chinese APT Groups,” 14 May 2019. (https://blogs.blackberry.com/en/2019/05/reaver-mapping-connections-between-disparate-chinese-apt-groups)

[87] Ibid

[88] Taiwan Presidential Election: A Case Study on Thematic Targeting https://pwc.blogs.com/cyber_security_updates/2016/03/taiwant-election-targetting.html

[89] APT1 Exposing One of China’s Cyber Espionage Units https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

[90] APT40：Investigations into Chinese government-sponsored spy groups. https://www.fireeye.com/blog/jp-threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html

[91] V. Gerasimov, 2013, Ценность науки в предвидении, Military-Industrial Kurier. (Robert Coalson, trans., 2016, The Value of Science is in Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations, the Military Review.)

[92] J. Berzins, 2014, “Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy,” National Defence Academy of Latvia Center for Security and Strategic Research. pp. 1–13.

[93] Janne Hakala and Jazlyn Melnychuk, RUSSIA’S STRATEGY IN CYBERSPACE, NATO STRATCOM COE, 2021.

[94] Major C. Kamphuis BSc., 2018, “Reflexive Control: The relevance of a 50-year-old Russian theory regarding perception control,” Militaire Spectator. (https://militairespectator.nl/artikelen/reflexive-control)

[95] A. Kowalewski, 2017, “Disinformation and Reflexive Control: The New Cold War,” Georgetown Security Studies Review. (https://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/)

[96] The following five paragraphs refer to and summarise this paper; Takahiro Tsuchiya, 2015, Neuro Security“Brain Supremacy” and “Mind Wars,” *KEIO SFC JOURNAL* Vol.15 No.2, 12-31.

[97] Michael N. Schmitt (ed.) and Liis Vihul (ed.), 2017, Tallinn Manual 2.0 on the Interna-tional Law Applicable to Cyber Operations. Cambridge University Press, Cambridge.

[98] *Ibid.*, pp17 ff..

[99] *Ibid.*, pp168 ff..

[100] ODNI, *supra* note7.

[101] Estonian Foreign Intelligence Service, 2019, INTERNATIONAL SECURITY AND ESTONIA 2019,

Estonian Foreign Intelligence Service.
[102] “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).
[103] Schmitt, *supra* note14, pp312 ff..
[104] Typical example is as follows.
Jessica Brandt, How Democracies Can Win an Information Contest Without Undercutting Their Values, PCIO POLICY PROPOSAL, AUGUST 02, 2021. (https://carnegieendowment.org/2021/08/02/how-democracies-can-win-information-contest-without-undercutting-their-values-pub-85058)
[105] G7 DECLARATION ON RESPONSIBLE STATES BEHAVIOR IN CYBERSPACE, https://www.mofa.go.jp/files/000246367.pdf (last accessed 2020/2/17).
[106] The report of this section based on the following policy recommendation which the author participated in the project to publish.
SPF, 2022, “Prepare for Foreign Disinformation! -Threat of Information Manipulation in Cyberspace-” (https://www.spf.org/security/publications/20220207_cyber.html)
[107] Michael Conte, “US conducted more than two dozen cyber operations targeting foreign threats to the 2020 election,” CNN, 25 March 2021 (https://edition.cnn.com/2021/03/25/politics/us-cyber-operations-election-threats/index.html)
[108] The project identifies fact-checking projects in each country as follows: whether they 'examine statements by all parties and positions'; whether they 'examine individual claims and draw conclusions'; whether they 'identify sources of information and explain how they do this'; whether they 'disclose funding and affiliations'; whether they 'disclose the fact-checking project's main mission is news and information', 'whether the project is run by professional journalists or media organisations', 'whether the project is affiliated with an academic journalism education programme', and other diverse criteria to determine its record of activity and to be included in the database.
（Bill Adair, Mark Stencel, ”How We Identify Fact-Checkers, Duke Reporters' Lab, 22 June 2016” ［https://reporterslab.org/how-we-identify-fact-checkers/］）
[109] Rumor Control (https://www.cisa.gov/rumorcontrol)
[110] The Digital, Culture, Media and Sport Committee, “Disinformation and ‘fake news’: Interim Report,” 29 July 2018 (https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36302.htm)
[111] The Digital, Culture, Media and Sport Committee, Disinformation and ‘fake news’: Final Report, The House of Commons, 14 February 2019 (https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf)
[112] Edward Malnic, ”Britain to carry out ‘offensive’ cyber attacks from new £5bn digital warfare centre,” The Telegraph, 2 October 2021 (https://www.telegraph.co.uk/politics/2021/10/02/britain-capable-launching-offensive-cyber-attacks-against-russia/)
[113] Full Fact awarded $500,000 to build automated factchecking tools (https://fullfact.org/blog/2017/jun/awarded-500000-omidyar-network-open-society-foundations-automated-factchecking/)
[114] Anne Catherine-Stolz, “Germany: Facebook Found in Violation of ’Anti-Fake News‘ Law,” Library of Congress, 20 August 2019 (https://www.loc.gov/item/global-legal-monitor/2019-08-20/germany-facebook-found-in-violation-of-anti-fake-news-law/)
[115] GET YOUR FACTS STRAIGHT! (GETFACTS) (https://all-digital.org/projects/get-your-facts-straight/)
[116] Raquel Miguel, “The battle against disinformation in the upcoming federal election in Germany: actors, initiatives and tools,” EU Disinfo Lab, 24 September 2021 (https://www.disinfo.eu/publications/the-battle-against-disinformation-in-the-upcoming-federal-election-in-germany-actors-initiatives-and-tools/)
[117] Der Bundeswahlleiter, “Erkennen und Bekämpfen von Desinformation -Desinformation in Social-Media-Kanälen”(https://www.bundeswahlleiter.de/bundestagswahlen/2021/fakten-fakenews.html#b1f77833-c1f9-4167-9e83-51019b667552)
[118] Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, and Janaina Herrera, Iinformation Mnipulation: A Challenge for Our Democracies, CAPS (Ministry for Europe and Foreign Affairs) and IRSEM (Ministry for the Armed Forces), August 2018 (https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf)
[119] Europian Commission, “European Democracy Action Plan”

(https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en)

[120] European Union Agency for Cybersecurity, “ENISA makes recommendations on EU-wide election cybersecurity,” 28 February 2019 (https://www.enisa.europa.eu/news/enisa-news/enisa-makes-recommendations-on-eu-wide-election-cybersecurity)

[121] Factually (https://www.gov.sg/factually)

[122] Venessa Lee, “2 initiatives launched to help fight fake news, terrorism,” The Straits Times, 13 January 2019 (https://www.straitstimes.com/singapore/2-initiatives-launched-to-help-fight-fake-news-terrorism)

[123] 池 雅蓉（Chih Ya Jung）, ” Fighting disinformation in cooperation with citizens: Taiwan's diverse fact-checking initiatives,” FIJ, 16 October 2019.（https://fij.info/archives/3242）

[124] Daniel Funke and Daniela Flamini, A guide to anti-misinformation actions around the world. (https://www.poynter.org/ifcn/anti-misinformation-actions/)

[125] Global Cybersecurity Index (https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx)

[126] Global Cyber Security Capacity Centre – The CMM (https://gcscc.ox.ac.uk/the-cmm)

[127] S. Mori and A. Goto, “Reviewing National Cybersecurity Strategies,” J. Disaster Res., Vol.13, No.5, pp. 957-966, 2018.

[128] Ibid

[129] NSC, “National Security Strategy of Japan”, December 2022. (https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf)

[130] M. Tsuchiya, “Cybersecurity and Intelligence Agency,” International Politics, Vol.179, pp. 44-56, 2015.

[131] Council of Parties on Internet Election Campaigning, “Guidelines for the Revised Public Office Election Law,” 2013. (https://www.soumu.go.jp/main_content/000222706.pdf)

[132] Ministry of Internal Affairs and Communications,” Final Report of the Study Group on Platform Services”, March 2022. (https://www.soumu.go.jp/main_content/000668595.pdf)

[133] The judgment states that the customs authorities are deprived of the opportunity to come into contact with the content of the ideas expressed in the relevant expressive material in Japan, thereby restricting the right to freedom of knowledge, and that even if customs inspections are not prior regulation themselves, it cannot be denied that they have aspects of prior regulation, and special consideration is required when determining the constitutionality of customs inspections. Special consideration is required in determining constitutionality. It is important to note that the Court argues that special consideration is required in determining the constitutionality of customs inspections. (Summarized and translated from 木下昌彦、片桐直人、村山　健太郎、横大道聡、西貝小名都、御幸聖樹、山田哲史・編、2018『精読憲法判例［人権編］』弘文堂．p277.)

[134] The discussion in this section bases on the policy recommendation of the Sasakawa Peace Foundation in 2022 “Prepare for Disinformation by Foreign Actors! -Threat of Information Manipulation in Cyberspace-” which I partly wrote. (https://www.spf.org/security/publications/20220207_cyber.html)

[135] Representative discussions are as follows.

J. Brandt, “How Democracies Can Win an Information Contest Without Undercutting Their Values,” Carnegie Endowment for International Peace, 02 August 2021. (https://carnegieendowment.org/2021/08/02/how-democracies-can-win-information-contest-without-undercutting-their-values-pub-85058)

[136] L. Seebeck, E. Williams and J. Wallis, “Countering the hydra : a proposal for an Indo-Pacific hybrid threat centre,” Australian Strategic Policy Institute, 07 Jun 2022. (https://www.aspi.org.au/report/countering-hydra)

[137] Ministry of Foreign Affairs of Japan, “Address by Prime Minister Shinzo Abe at the Opening Session of the Sixth Tokyo International Conference on African Development (TICAD VI)”, 27 August 2016. (https://www.mofa.go.jp/afr/af2/page4e_000496.html)