Title	Chapter 3-III : ‘Weaponization of data’ and the rise of DPFs in security : is Mechagodzilla a friend of mankind?
Sub Title	
Author	Fuse, Satoru
Publisher	Keio University Global Research Institute
Publication year	2025
Jtitle	Monsterizing Platform Power and Law ; Volume 1. Platforms and States: How to Settle the Battle of Monsters ,p.141- 152
JaLC DOI	10.14991/KO11003002.00000001-0141
Abstract	
Notes	Chapter 3 : The field of attack and defense over the governance of digital space
Genre	Book
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO11003002-00000001-0141

Chapter 3 - III

'Weaponization of Data' and the Rise of DPFs in Security

: Is Mechagodzilla a friend of mankind?

Satoru Fuse*

Introduction

Amazon, Google, X (formerly Twitter), YouTube, and Facebook. Not a day goes by without using the services provided by the Digital Platformer ("DPF").[1] The DPF service has become so ingrained in our daily lives, but did you know that it continuously collects data about us?

For instance, a Google search stores information on the DPF side about your interests, what you want to buy, where you are thinking of going, when and where you looked it up, and so on. If you are logged in with a Google account, the demographic information you have registered, e.g. your gender, age, and location, will also be included. Every day, a huge and continuous amount of data about you is collected. It may be Google, not your spouse, who understands you best.

The use of such data is also spreading into the area of security; the era of waging war and doing business using data has arrived. As the strategic importance of data increases, the presence of DPFs, which collect, store, and utilize data on a large scale and continuously, is growing, and in military and intelligence, states are even becoming more dependent on DPFs.

This chapter will focus on the growing importance of such data and the rise of the US DPFs in the national security domain and analyze how the Japanese Government will build a cooperative framework with the giant DPFs from in and outside of Japan for national security in the future.

(1) Micro-targeting as data utilization

Have you heard of the technique of micro-targeting? It is heavily used in digital business by collecting

* **Satoru FUSE:** Project Professor specialized in Economic and National Security at SHINSHU University, Executive Chief Fellow at the Institute for International Socio-Economic Studies (IISE) and Visiting Fellow in the Command and Staff College at the Japan Maritime Self-Defense Force.

1 In this chapter, DPFs include Google, X (formerly Twitter), Meta (formerly Facebook), Microsoft, Yahoo Line and other major Japanese and US companies that collect, store, analyze and utilize large amounts of user data daily by operating search, social media, message applications and cloud-based businesses.

user data such as who they are connected to, what they have bought in the past, what sites they have visited, how long they have stayed, and what their demographics are, to present advertising that is relevant on a personal level to encourage them to buy.[2]

Internet advertising using micro-targeting analyses the interests and concerns of users based on those data and delivers advertisements that match them. In general, the length of time spent on a particular site, click history, location information such as IP address, purchase history, information identifying the device and browser, and keywords searched for are often acquired and used by operators.

By displaying or sending advertisements, messages, or narratives that conform to the preferences of the target individual, the aim is to influence their thoughts and behavior (such as voting or purchasing behavior, preferences) and to steer them in the direction desired by companies, governments, or candidates.

In the US, this approach has been applied to political campaigning strategies. By profiling people such as "a woman with a university degree who lives in the suburbs, has children and whose children attend soccer classes", and analyzing what policy interests them, or more specifically, what they expect to hear. Based on such information, candidates convey the issues and messages that such voters want to know about, aiming to encourage support and voting behavior. Those women are commonly known as 'soccer moms' among US election experts, regarded as key swing voters who will decide the presidential election. They are considered to be highly interested in everyday issues such as the economy, education, and city security, known as 'kitchen table issues'. Based on such analysis, candidates campaign on the worsening city security caused by illegal immigration and attack the Democratic candidate who is more tolerant of immigrants.

What makes this possible is data. This can only be achieved by acquiring, accumulating, and analyzing (utilizing data) a vast amount of data that enables accurate analysis of what the user's attributes are, and what they think and want as if looking inside their heads. In the business world, the company that can perform this cycle accurately and speedily will determine its superiority in the market.

A successful example of this is SHEIN, a fashion e-commerce site from China that is extremely popular among young women and sweeping the world. The strength of SHEIN, which has more than 43 million users worldwide, is its speed and abundant product line-up. It only takes as little as three days from development to commercialization, which is faster than other 'fast fashion' sites such as ZARA, and quickly grasps the latest trends demanded by consumers and commercializes them. This 'real-time fashion' company[3] is far ahead of its competitors in terms of the speed and cycle of developing products, and the number of products released reaching 10,000 items every month. SHEIN has many strengths, such as shortened manufacturing processes, in-house design, tactical advertising and promotion by influencers and TikTok, and low prices that are favored by the savings-minded Generation Z. The foundation of its success is the use of data.

AI analyzes user preferences and purchasing behavior in real-time, such as what products users are searching for, whether they put them in their shopping carts, what products they put in their carts but did not

2 Michael Smiley, "What is microtargeting and what is it doing in our politics?" 4 October 2018, https://blog.mozilla.org/ en/products/ firefox/microtargeting-dipayan-ghosh/

3 Daxue Consulting, SHEIN's Market Strategy: How the Chinese Fashion Brand is Conquering the West, 6 July 2022, https:// daxueconsulting. com/shein-market-strategy/

purchase, and what products and designs are generating buzz on social media.[4] Based on the data, products incorporating the latest fashion trends are introduced. Even after the products are sold, user search and purchasing behavior are monitored to identify popular trends. If the demand for the product is still high, the number of products produced can be increased at any time.

Micro-targeting, which utilizes such data to encourage behavioral and thought (and preference) changes in consumers, has also been applied to military and intelligence operations, and data utilization is also advancing in national security.

(2) Data to be weaponized

In the business world, data utilization is used to understand consumer preferences and tastes, similarly, in the military intelligence world, it is used as a weapon to understand the weaknesses of an adversary. The more relevant and detailed information they have, the better they understand the target's weaknesses.

A case that illustrates the importance of data in the intelligence domain is the US Federal Office of Personnel Management data breach (OPM hacking case) in 2015. China is suspected to have been involved in the incident, in which more than 21 million personal data of US federal government employees were compromised in a cyber-attack.[5]

The data breach included information that is required during the screening process to obtain a security clearance, and it is believed that information on current and former intelligence agency personnel and their spouses was leaked to the Chinese side. This included fingerprint data for 1.1 million people. Due to this data breach, it is reported that CIA personnel and others engaged in clandestine operations abroad were sent home urgently or were prevented from working in the field to avoid the risk of their identity being exposed.[6]

When applying for a security clearance, which will allow them to access classified information or restricted areas, they are required to fill out a 133-page application form called the SF-86, detailing their drinking history, financial situation, assets, foreign friends, foreign travel history, criminal record, drug use history, and marital status, etc.[7] In the eyes of foreign intelligence agencies, it is a treasure trove, as it provides information on debts, affairs, friendships, foreign connections, and other potential weaknesses of the target, making the recruitment of spies dramatically efficient.[8] A senior US intelligence official who assessed the impact of the OPM data breach said: "The work took an inordinate amount of time. The scale of what the Chinese intelligence agencies were able to ascertain from the data they obtained was nauseating".[9]

4 Sgentbox, 'What is the fastest growing fashion brand SHEIN?' 8 Aug 2023. Available at: https://scentbox.jp/shein-ai/ SHEIN's privacy policy lists includes 'your preferred style', 'location data based on IP address' and 'data about your use of the service (browsing, adding to shopping cart, securing products, ordering and returning)'. SHEIN Privacy Policy, 'Our Collection and Use of Personal Information' (effective 17 February 2022), https://jp.shein.com/Privacy-Security-Policy-a-282.html

5 Kristin Finklea, Michelle Christensen and Eric Fischer, Cyber Intrusion into the U.S. Office of Personnel Management, (Congressional Research Service, July 17, 2015).

6 Ellen Nakashima and Adam Goldman, "CIA Pulled Officers from Beijing After Breach of Federal Personnel Records," *Washington Post*, September 15, 2015.

7 US Office of Personnel Management, Standard Form 86-Questionnaire for National Security, https://www.opm.gov/forms/pdf_fill/sf86.pdf

8 War on the Rocks, "The 9 Scariest Things That China Could Do With The OPM Security Clearance Data," 2 July 2015.

9 Zach Dorfman, "Tech Giants are Giving China a Vital Edge in Espionage," *Foreign Policy*, 23 December 2020.

AI enabled the utilization of the vast amounts of data allegedly obtained by China: in 2015, advanced and sophisticated algorithms that could analyze big data on 20 million people and suggest the best vulnerable targets for recruiting as informant were not yet at a sufficiently practical stage. They were sitting on a huge amount of data gold mine, however, the emergence of AI finally allowed them to mine gold.

Adam Kozy, a former FBI, and CEO of cybersecurity firm SinaCyber stated in testimony before the US Congress that "Chinese intelligence agencies are integrating data obtained through OPM and theft through other means in order to conduct espionage and select targets for cyber-attacks"[10].

There is a persistent view in the US that this is made possible by public-private partnerships between Chinese intelligence agencies and China's giant DPFs, in addition to the practical application of AI-based analysis. China's National Intelligence Law mandates Chinese companies and individuals to cooperate in intelligence activities, and it is believed that Chinese DPFs, telecommunications companies, and cybersecurity firms are ordered to cooperate, allowing Chinese intelligence agencies to use the computing infrastructure and data centers held by these companies.[11] "Chinese tech companies play a central role in analyzing vast amounts of data and making it available for use" (William Evania, former US Director of National Intelligence). He claims that the data stolen in the OPM hacking case was analyzed and used for intelligence activities within the framework of such "public-private cooperation".[12]

Another example of the utilization of data in intelligence operations is the acquisition of Grindr, one of the world's largest LGBT social apps. Grindr is a so-called LGBT matching app with 3 million daily active users. It collects a wide range of personal information, from the messages and location of users to their HIV status if they have chosen to make their information public.

Grindr was acquired by a Chinese gaming company between 2016 and 2018, however, the Committee on Foreign Investment in the United States (CFIUS), which reviews foreign investment in the US from a security perspective, ordered the Chinese company to sell Grindr in March 2019; demanded the divestment of a company. Why did the US government take the unusual step of ordering an already completed acquisition deal to a clean slate?

Grindr users include US government officials and US military personnel, and it is believed that there was concern that sensitive personal information such as sexual orientation and HIV status could be used to blackmail them when recruiting intelligence asset.[13]

The OPM case and Grindr acquisition case indicate the 'weaponization of data', big data - the vast amounts of personal data collected and stored - is weaponized by hostile states and used for activities detrimental to their national security. Micro-targeting methods provide a business personalized advertising and marketing

10 Adam Kozy, Testimony before the U.S.-China Economic and Security Review Commission Hearing on "China's Cyber Capabilities. Warfare, Espionage, and Implications for the United States", https://www.uscc.gov/sites/default/files/2022-02/Adam_Kozy_ Testimony.pdf

11 2022 Annual Report to Congress of the U.S.-China Economic and Security Review Commission, November 2022, pp. 419, 449-450, 456.

12 Dorfman, *Foreign Policy.*

13 Yuan Yang and James Fontanella-Khan, "Grindr Sold by Chinese Owner after US National Security Concerns," *Financial Times,* March 8, 2020.

tool, however, such methods are perceived as a weapon in the security world.

(3) The rise of US DPF in national security - deepening cooperation with the US Government

As the 'weaponization of data' progresses, in which large amounts of data are collected and accumulated and utilized as a means of securing a state's advantage, it is not surprising that DPFs with expertise in data analysis methods and utilization of such data will play key roles. Currently, the cooperation between the US Government and the US DPFs in national security is growing deeply.

The depth and scale of the cooperation between the huge US DPFs, known as GAFAM, and the US Government, especially the US military, is beyond our imagination, and we are keenly aware that the US DPFs have a different perspective from the one we perceive in our daily lives. It is no exaggeration to say that the US military can no longer fight future wars without cooperation with the DPFs.

It is AI and data that are linking the US military and the DPFs. The US military is promoting the military digitalization as a reform for the future of warfighting. A defense cloud infrastructure called JWCC (Joint Warfighting Cloud Capability) and a command-and-control network supporting system, JADC2 (Joint All-Domain Command and Control: Integrated Cross-Domain Tactical Command and Control System) are the two pillars of digitalization of the US military for future warfare.

JADC2, one of the two pillars, is characterized by the accumulation in the cloud of large amounts of data not only from the land, sea, and air space but also from the cyber domain. AI analyzes the situation and suggests possible options faster than human cognitive capacity. The aim is to accurately assess the situation faster than the enemy and move to attack first; to win through 'superiority in decision-making'.[14]

AI is key to this 'superiority of decision-making', which the attempt of US military to achieve through digitalization. AI will be a core technology of the JADC2 initiative, and Google is participating in this AI development project.[15]

As some readers may already be aware, collecting a large amount of data to understand the latest situation, which is then analyzed by AI to derive possible actions and take to next steps. Maximizing the speed of this cycle to gain an advantage over the competition. Such utilization of data is already conducted by the Chinese fashion e-commerce site giant SHEIIN. It is worth noting that the two organizations from the US and China in completely different domains have reached almost the same conclusion on how to utilize data.

JWCC, the Defence Cloud, on the other hand, will be the data infrastructure supporting JADC2, a command-and-control network that utilizes data to conduct operations.[16] The DoD has already signed a $9 billion

14 Fuse, Satoru, 'US Forces Advance Digitalization and the Future of Warfare', Monthly Voice (June 2022 issue, PHP Research Institute).

15 Jackson Barnett, "Northern Command Calls Upon Palantir, Apple and Others to Bring New Tech to Coronavirus Fight," *FEDSCOOP*, May 13, 2020, https://fedscoop.com/northern-command-apps-palntir-apple-covid19/

16 Mark Pomerleau, "Forthcoming JWCC Enterprise Cloud Will Be Key to Enabling JADC2, DOD CIO Sherman Says," *DefenseScoop*, November 9, 2022, https://defensescoop.com/2022/11/09/forthcoming-jwcc-enterprise-cloud-will-be-key-to-enabling-jadc2-dod-cio-sherman -says/

contract with Amazon AWS, Microsoft, Google and Oracle.[17] The cloud is the foundation for the collection and aggregation of data, and since the JADC2 is aimed at data-driven warfare and handles large amounts of data, the cloud infrastructure that serves as the platform for this can be considered the core of US military digitalization. Google, Microsoft, and Amazon are involved in the infrastructure development of such core technology.

AI and cloud computing support digitalization, which is key to the US military's future warfighting strategy, and both of which involve the US DPFs (GAFAM). Especially when it comes to cloud infrastructure, it would not be possible without the participation of DPFs, which have overwhelming technological knowledge and market dominance in the cloud business.

Cooperation between the US Government and the US DPFs (GAFAM) in national security is not limited to the military domain. Cooperating agencies range from law enforcement agencies such as the FBI and police to intelligence agencies such as the CIA, and the topics of cooperation are also broad; from monitoring domestic extremist groups on the internet, counter-terrorism, counter-election intervention, counter-disinformation, and cyber-attacks.[18]

Due to their influence, the role played by the DPF is becoming comparable to that of the state. In counter-terrorism, the DPFs have a blacklist of organizations and individuals suspected of involvement in terrorism, which is similar to a government sanctions list. It also plays an important role in the prevention of foreign intervention in elections by protecting the democratic process through information exchange with law-enforcement and intelligence agencies. DPF, which monitors its cyberspace, detects and responds to intelligence activities such as foreign influence operations and disinformation dissemination, and even notified the US Department of Defense after the (then) Facebook blocked a large number of fictitious accounts created by the US military for their information operations abroad.[19]

Today, presence in cyberspace has the same value and meaning as physical presence in real space. It is no exaggeration to say that if companies or politicians are not allowed to be on the internet, it is nearly synonymous that they do not exist in the real world.

In this sense, the DPF's power to block accounts can be considered as the power to control one's life on the internet, which is equivalent to state recognition by a government. Twitter (now X) demonstrated its power at the time with the permanent suspension of former President Trump's official account. It was undoubtedly a major blow to Trump, whose method of using Twitter to deliver messages directly and at will to his supporters without the filtering of the major media was a main source of his political influence.

In the Biden administration's withdrawal of US troops from Afghanistan in August 2021, the decision by Facebook (then), Google, and Twitter (then) proved to have an impact equal to that of the government. The US government was faced with a decision on whether to officially recognize the Taliban, which was taking control of Afghanistan after the withdrawal of US troops, as the Afghan government. Similarly, the

17 U.S. Department of Defense, Immediate Release, Department of Defense Announces Joint Warfighting Cloud Capability Procurement, Dec 7, 2022.

18 Elena Chachko, "National Security by Platform," *Lawfare*, Dec 8, 2021.

19 Ellen Nakashima, "Pentagon Opens Sweeping Review of Clandestine Psychological Operations," *Washington Post*, Sep 22, 2022.

public policy directors of the three US DPF companies were also under pressure to decide whether to allow the Taliban to take over the official Afghan government account, meaning allowing the Taliban to use US DPF services to communicate with and govern the Afghan people.[20] Allowing the Taliban to manage the official accounts of the Afghan government, including the account of the Afghan president, had the equivalent political effect of formally recognizing the Taliban government.

Ultimately, they did not authorize the Taliban to manage those accounts based on a code that prohibits the use of organizations involved in terrorism. However, this story indicates how the DPFs are becoming so influential and powerful in national security.

The development of public-private cooperation between the US Government and the DPFs has also led to increased personnel exchanges. The former Facebook, Google, and Twitter (now X) have all strengthened their departments related to national security and geopolitical risks, and the recipients of the supply of personnel for these departments are the US intelligence agencies and the US military. Facebook, in particular, has tripled its 'trust and security' related personnel since 2016, strengthening its staff to 40,000 (in comparison, the number of US diplomats is 15,600).[21]

Google has also established a new department to counter state-sponsored cyber-attacks, the Threat Analysis Group (TAG), which is led by a former Australian intelligence executive. With a large number of former government officials, TAG is believed to be the largest counter-intelligence operation by a private company and is also referred to as a 'small intelligence agency'.[22] The data is not the latest, however, between 2007 and 2016, Google hosted 251 former US federal government employees.[23]

If data-driven, such as digitalization and the use of cloud promoted by the US military, becomes the premise, DPFs with such technology and know-how will be valued, and the US government will become dependent on DPFs (the cloud is a prime example).

The more advanced the technology, such as AI or cloud computing, the less the 'client' (the government) can technically verify the 'developer' and 'provider' (the DPFs). Likewise, the more advanced the specific technology, the higher the barriers to entry or the less substitutability by other operators, forcing the government to rely on the existing operators (the DPF) and traps into so-called vendor lock-in.[24]

In particular, if the government is dependent on the technology of DPFs and specific operators not only for the planning of military operations and intelligence gathering but also for the actual execution of military operations in the field itself, such as JADC2, DPFs could even become involved in the ultimate exercise of national sovereignty in the use of force.

20 Cristiano Lima, "The Technology 202: Facebook, Twitter, YouTube face High-Stakes Question of Whether to Recognise Taliban.," *Washington Post*, Aug 17, 2021.

21 Joshua Fruhlinger, "Facebook Ramps Up Hiring for Privacy, Security and Trust Related Jobs," *B2 The Business of Business*, May 2, 2019, https://perma.cc/4h7X-PMUD

22 Robert McMillan, "Inside Google's Team Fighting to Keep Your Data Safe from Hackers," *Wall Street Journal*, Jan 23, 2019.

23 Tech Transparency Project, Google's US Revolving Door, 26 April 2016.

24 Majority Staff Report and Recommendations, Investigation of Competition in Digital Markets, Subcommittee on Antitrust, Commercial, and Administrative Law of the Committee on the Judiciary of the House of Representatives, October 2020, p. 98.

(4) How should Japan face the DPF?

In this final chapter, I would like to conclude by considering the possibility and challenges of public-private cooperation between the Japanese government and DPFs in Japanese national security. The famous DPFs active in Japan are the US-based GAFAM and the former Yahoo!JAPAN (now LINE Yahoo) is a domestic company. National security cooperation between the Japanese government and DPFs has never been as full-fledged as it is in the US.[25]

On the other hand, if the Japan Self-Defense Forces (JSDF) decides to pursue digitalization and data-driven operations in the future, there could be possibilities to move towards collaboration and cooperation with the DPFs, which are skilled in the use of data. For instance, the Air Self-Defence Force is moving forward with plans to migrate to a third generation of cloud infrastructure; as of October 2023, Amazon's AWS is being considered as one of several vendors, and if digitalization advances in the JSDF in the future, collaboration with the US DPFs may deepen, as it did in the US.

The most likely cooperation between the Japanese Government and the DPFs in the near future will be against disinformation and influence operations.[26] In the National Security Strategy, the Government of Japan has repeatedly mentioned disinformation by foreign powers and has expressed its concerns.[27] The government has set up a system for the International Public Relations Office of the Prime Minister's Office, the Ministry of Defence, the Ministry of Foreign Affairs, the Ministry of Internal Affairs and Communications, the National Police Agency, and others to set up new departments in charge of disinformation under the lead of the Cabinet Intelligence and Research Office.[28]

Disinformation is one of the means of influence operations can be carried out both openly and covertly. There is concern that the comment sections of social media and news websites by DPFs may become the main battleground for the spread of disinformation (influence operations).

China places great emphasis on influence operations. In its ideological struggles, China emphasizes the idea of the 'right to speak', i.e. the power to create narratives, or discourses, and have them accepted by foreign countries.[29] In the Taiwan issue (Taiwan contingency), which China positions as a core interest, there is concern that China will try to steer global public opinion in the direction they desire or disrupt de-

25 For example, the former Yahoo! Japan works with law enforcement agencies such as the police in responding to requests for disclosure of user information for the purpose of criminal investigations. There is a certain level of cooperation between the DPF and authorities in criminal investigations, https://about.yahoo.co.jp/pr/release/2021/07/ 28b/

26 Influence operations, disinformation, information warfare and cognitive warfare are interrelated, however, there is no unified definition yet. For the purposes of this chapter, influence operations are defined as activities to influence government leaders, public perception and decision-making, and to disrupt or steer regimes and decision-making in a desired direction. It is carried out in both peacetime and contingency and may be combined as a military tool as part of a military operation, or may be envisaged as a non-military tool, such as election intervention, and carried out separately from military operations. Most influence operations are often conducted in combination with cyber-attacks. Strategic-level activities that disrupt operational behaviour by influencing the decision-making and perceptions of enemy commanders and soldiers on the battlefield are not discussed in this chapter. The spread of disinformation is one of the means of influence operations, which should be positioned as a higher-level concept of disinformation spread. However, this chapter regards influence operations and disinformation spread in the equal position for the reader's understanding.

27 Cabinet Secretariat, National Security Strategy, 16 December 2022, pp. 7, 24, 30.

28 'Strengthening measures against disinformation: systems in place in the Cabinet Secretariat,' *Nihon Keizai Shimbun*, 14 April 2023.

29 Meiko Eto, 'China's conflict over universal values', *Agilent World Trends*, no. 266, Dec 2017, pp. 26-33.

cision-making by the Japanese and US governments and public opinion, through a mixture of correct and false information.[30] If, as the situation in Taiwan becomes increasingly tense, influence operations targeting Japanese policymakers and public opinion are carried out, it will be essential to build cooperation with the DPFs, which operate social media and internet platforms that serve as channels for the transmission of disinformation and narratives. Countering influence operations in the event of a Taiwan emergency will be a touchstone for the Japanese Government, testing the nature of public-private cooperation with the domestic and international DPFs.

Tracking online disinformation tends to focus on detection techniques, however, a more important step is the response after detection. To counteract the effects of disinformation, it is essential to immediately develop a counter-narrative and to publish, report, and disseminate accurate facts. If such responses are delayed, the disinformation may be seen by many people online and may remain influential. In that case, no matter how many deletion or non-display measures are taken afterward, spreading disinformation will have been achieved.

For a rapid response to such a situation, it is essential that the government, which detects false information, and the DPFs, which have platforms where information circulates such as social media and internet platforms, work together to take measures to delete or moderate problematic posts and disinformation. Considering the speed at which information spreads in the internet space, it would be desirable to automate certain processes such as detection by the government, communication to the DPF, the decision on whether the DPF should take action or not, and implementation of the action. Prior communication between the government and the DPFs is essential, including the establishment of a response procedure, implementation of response criteria, and consideration of legal issues, however, full discussions on the issues involved in such anti-disinformation measures, the division of roles between the government and the DPFs, and the nature of the cooperation system, have not yet started.

How far will the DPFs cooperate?

The particular concern in this cooperation with DPFs in countering disinformation is which foreign DPFs will cooperate for national security emergencies in Japan, such as the Taiwan contingency. In general, it is probably the common understanding that all private operators, whether domestic or foreign, do not welcome requests, regulations, or interventions from the government to a greater or lesser extent.

30 The National Institute for Defence Studies report introduces a scenario predicted by the Taiwanese authorities that China is conducting influence operations such as the spread of fake news are deployed in combination with other military operations to 'win without a fight' in its invasion of Taiwan. Shinji Yamaguchi, Masaaki Yatsuzuka and Rira Monma, China Security Report 2023, National Institute for Defense Studies, pp. 43-53. The US State Department has described China's global information operations, including disinformation and propaganda, as a 'challenge to the integrity of the global information space,' and noted that they could 'spread scenarios that is favor to the Chinese government' and 'influence economic and security decisions in favour of China' on the Taiwan issue. U.S. Department of State, Global Engagement Center Special Report: How the People's Republic of China Seeks to Reshape the Global Information Environment, 28 September 2023.

It is easily expected that foreign DPFs operating globally would not have the incentive to allocate more resources or to take a carefully tailored approach to Japan alone, which is only one of many markets. The Japanese Government will be required to become a skilled "Lion tamer" in order to elicit timely and effective cooperation with the giant foreign DPFs.

The EU is clear on this point. The EU, which does not have large international DPFs, is not required to focus on the protection of its own DPFs and is taking a detached approach, using regulation and legally binding force as the whip to influence the large DPFs i. For example, the EU has called on Meta and X to take action within 24 hours on the spread of disinformation online over the clashes between Israel and Hamas and has launched an investigation into X.[31] The Digital Services Act (DSA) allows to take such action. It requires the DPF to crack down on harmful content and disinformation and can impose fines of up to 6% of global sales if it considers the response insufficient. This powerful regulation, which in the worst-case scenario could even require the DPF to withdraw from the European market if the problem is not remedied, makes the demands on the DPF more effective and serious.

While minimum government regulation and intervention is ideal for the sake of free competition, the free use of the Internet, and active innovation, it must be emphasized that expecting the DPFs to take voluntary and autonomous measures against disinformation during national emergencies and contingencies leaves challenges to its effectiveness. It will be an important issue to what extent the EU model, which is based on a certain degree of legally binding power to elicit cooperation rather than expecting voluntary actions from DPFs, is adoptable into the design of public-private cooperation with DPFs in Japan in the future.

The national security risks associated with services provided by DPFs such as social media and search, should also be taken into account when considering the regulations on DPFs. In particular, search engines (and the generative AI implemented in them) provided by national and international DPFs are useful tools, however, these can also be a perfect means of influence operations if misused by malicious actors.

In national security, the concept of cognitive warfare has been attracting attention. It aims to confuse or control decision-making and public opinion in a target country by disseminating specific narratives to the political leaders and citizens. The spread of disinformation and influence operations, which we discussed in this chapter, are one of the tools of this cognitive warfare.

If malicious actors were able to control search engines, they could understand what users are thinking and looking for from their search terms. Combined with the location of the user, this would increase the resolution of what is being searched in a particular location in Japan. If the search term 'JSDF defense deployment conditions' increases in the area of the House of Representatives building and the Prime Minister's office, it can be inferred that some sort of Self-Defence Forces deployment is being considered.

It can also be applied to election analysis. For example, if the keyword 'Innovation Party' increases in the Hokkaido area during the election period, it would indicate that interest in the Innovation Party, which has

31 X responded that the accounts and posts by the terrorist organization and others has been blocked or deleted. Meanwhile, Meta claims that a team including experts in Hebrew and other languages monitored the site 24 hours a day, and that over 790,000 posts were deleted or labelled with a warning in the three days following the attack. https://www.nikkei.com/article/DGXZQOGN128DW0S3A011C2000000/

its support base mainly in the Kansai and Tokyo metropolitan areas, is spreading widely to other regions, and it indicates that the 'Innovation Party' momentum is becoming a nationwide phenomenon. If it is possible to infer the interests and strategies of a particular Japanese company in a particular location from the content of their search, it is theoretically possible to conduct an industrial espionage-type operation to convey such information to foreign companies. In the extreme, being able to know the search terms means being able to peek into the thinking of the Japanese.

The national security risks of foreign-origin search engines (especially those from countries other than the US) in Japan are issues that should be discussed in detail. This is because understanding what the Japanese are searching for or what they are expecting allows us to explore touchpoints to see what topics and narratives can influence the Japanese. In other words, it can be a preparation for influencing and guiding operations (influence operations), as well as an intelligence analysis of what is happening in Japan.

Not only that, but search engines can also be a mechanism for how to make people change their thoughts and behavior. Based on search terms, known as search queries, search engines crawl the internet to gather the information users are looking for and display the search results. It is no exaggeration to say that the user perceives the world through the information presented in a way that personalizes the user's interests.[32] If those controlling search engines can manipulate the search results display algorithms, they can also manipulate the output of the search results, and therefore they may be able to transform the perceptions and behavior of their users/targets.

For example, if users are repeatedly imprinted by displaying 'Russian territory' instead of 'Japan's inherent territory' when searching for 'the Northern Territories', some people's perceptions of the Northern Territories may be affected in the long term. In the case of the Taiwan contingency, there is concern that false information and narratives such as 'the US will abandon Taiwan and Japan' may be spread on social media, short videos, and search results and that may induce a mood of war-weariness in Japanese public opinion.

We are unconsciously influenced in our thinking and behavior by the search engine results we casually use every day - what and how we perceive it, what we buy, where we go and don't go. If the search engine is operated by a country of concern, a non-aligned country, or even within a country under the influence of malicious actors, we may unknowingly be under the influence of operations and manipulation of public opinion. How to incorporate such risk mitigation measures into government/DPF cooperation is an extremely important issue.

Conclusion

The giant DPFs accumulate and operate large volumes of data, which can be regarded as modern strategic assets. Today, their presence is no longer limited to the business but is also expanding in the national security

32 The Committee on the Judiciary of the House of Representatives, pp. 61-66.

domain. In the US, the institutionalization of public-private cooperation is progressing, with the military, intelligence agencies, and the giant DPFs increasingly interacting and trading with each other, and in some areas, the government even relies on the DPFs.

A 'cooperative model' of public-private partnership is emerging in the US, where the government and the DPF form a strategic partnership, to jointly address national security challenges. These trends are likely to intensify as digitalization and data utilization in the national security domain progress. In the future, momentum for public-private cooperation between the government and DPFs in countering disinformation will increase in government and society (regardless of the DPF's intentions) while people become more aware of the dangers of a Taiwan contingency.

The government needs information, analysis, and cooperation from the DPFs[33]. In the EU model, the DPFs are obliged to cooperate and work together with a legally binding background, however, in the 'agreement model', the government is in the position of 'asking' for the corporation. It is doubtful that the DPF is strongly incentivized to cooperate with the government, as it is not necessarily directly linked to profits, but rather a "social responsibility". It will be a major challenge to face how much cooperation can be obtained from the DPF on a 'request' basis.

Furthermore, as digitalization and data utilization in the JSDF progresses, there is no doubt that Japan, like the US, will deepen its cooperation with the giant DPFs. However, as the 'agreement model' is based on the assumption that the government and the DPFs will build an equal cooperative relationship, it is important to maintain a balance to ensure that the government is not overly dependent on the DPF, thereby strengthening the DPF's negotiating power in the national security field and weakening the power of government.

The DPF may have an influential voice and negotiating power due to the high technical barriers to the use of cloud infrastructure and data. The Japanese Government is required to have the technical knowledge to accurately assess the explanations and proposals by DPFs. There is no guarantee that the DPF will always respond to the requests by the Japanese Government on a priority basis, despite prompt and timely response being essential for disinformation measures. To build equal and functioning 'agreement model' partnerships, the government is required to have a certain level of technical knowledge and be able to exert a check-and-balance effect on the DPF with a certain degree of legally binding force.

33 Tatsuhiko Yamamoto, 'Form Strategic Relationships with Platforms,' *Voice*, June 2020, PHP Research Institute.