Emergence of "State-Centrism" in Cyberspace*

Takahisa Kawaguchi**

Abstract

There was a time when cyberspace was regarded as a utopia. The emergence of cyberspace centered on the Internet and the expansion and deepening of digital space were expected to greatly change the established system of sovereign states. Because cyberspace was to have no national boundaries, it would relativize the power of sovereign states and lead to a decrease in international conflicts. Today, however, as there are clear national boundaries in the "flow" and "stock" of digital information, it is sovereign states that have the most sophisticated cyber capabilities, and the major powers are engaged in conflict in cyberspace and regarding cybersecurity. The ongoing conflict between the US and China over technological superiority and the dispute regarding Russian interference in US elections are problems borne from the expansion and deepening of cyberspace. "State-centrism" is expanding in cyberspace in the sense that sovereign states exercise power centered on their national security and strategic competition.

Introduction

Cyberspace—that is, networks to transmit, exchange, and share digital information—is continuing to expand.[1] In this process, cyberspace has penetrated every aspect of society and daily life, and brought about changes in communications, industries, the formation of social consensus, and all other fields.

Then, what types of changes is the expansion and deepening of cyberspace causing in global politics and international relations? How should we grasp global politics and international relations in cyberspace?

In its earliest stages, cyberspace was perceived as a utopia; because cyberspace was to have no national boundaries, it would relativize the power of sovereign states and lead to a decrease in international disputes. Today, however, there are clear national boundaries in digital space, it is sovereign states that have the most sophisticated cyber capabilities, and the major powers are engaged in conflict in cyberspace and also regarding cybersecurity. The ongoing conflict between the US and China over technological superiority and the dispute regarding Russian interference in US elections are both confrontations that emerged because of the expansion and deepening of cyberspace.

In the sense that sovereign states exercise power centered on security issues and disputes

---

* This essay was originally published on *Kokusai Mondai* [International Affairs], No.683 (Jul.-Aug. 2019).

** Takahisa Kawaguchi is Principal Researcher at Research Institute for Strategic and Political Risks, Tokio Marine & Nichido Risk Consulting Co., Ltd.

1 Regarding the deepening and expansion of cyberspace, see Takahisa Kawaguchi, "Kawariyuku saiba kukan de no senso" [Changing war in cyberspace], in *"Gijutsu" ga kaeru senso to heiwa* [War and peace being changed by "technology"], ed. Narushige Michishita (Fuyo Shobo Shuppan, 2018), pp. 27–39.

between major powers sometimes arise, "state-centrism" is emerging in cyberspace. Cyberspace "is moving from its halcyon days as an ungoverned stateless commons with only technical supervision into a geopolitical arena of intense complexity."[2]

Such conditions may be called "a reversion to the world of classical realism."[3] In the world view of classical realism, the most influential actor is the sovereign state, and the state acts to survive and maximize its power. The most important issue is national security, and international politics is regarded as a power struggle.[4]

This does not apply only to cyberspace. The present international environment has been described as "the revenge of geography" (Robert D. Kaplan) and "a revival of Westphalian sovereignty" (Ian Bremmer): a world where the power game among sovereign states is being fully pursued.

This paper first summarizes cyberspace as a utopia, notes the misunderstandings and realities regarding national boundaries, power, and disputes in cyberspace, and lastly describes ongoing disputes in cyberspace among the major powers.

1. Cyberspace as a Utopia

There was a time when cyberspace was grasped as a utopia.

This cyberspace is comprised, at the very least, of (1) the Internet, (2) closed networks that are not connected to the Internet, and (3) computer terminals, servers, storage media, and other electronic devices that are (or can be) connected to the Internet and these other networks.

The Internet is the core element comprising cyberspace, but its history spans half a century at most (ARPANET, which is the predecessor to the Internet, established packet-switching links in 1969). The history of commercial use of the Internet is just 30 years long, and during that time cyberspace has transformed into a backbone supporting social infrastructure, home electronic devices, and the realm of speech.

It has been noted that the Internet was developed by the US Department of Defense, but that is not an accurate description. While the Advanced Research Projects Agency (ARPA; renamed later the Defense Advanced Research Projects Agency [DARPA]) certainly did have a major role in the development of the Internet, the operation of ARPANET was actually initiated by researchers at four universities centered on the west coast of the US.

The design concept for the Internet characterized as "autonomous," "distributed," and "collaborative" differed from traditional rule by government.[5] The emergence of cyberspace centered on the Internet, which has no national boundaries or central authority, demanded a re-evaluation of the roles of state and of government. John Perry Barlow, the founder of the Electronic Frontier Foundation, criticized legislation to regulate the Internet in the US (the Communications Decency Act) and published "A Declaration of the Independence of Cyberspace" on February 8, 1996. Barlow argued that cyberspace is a sovereign space where governments

---

2 Parag Khanna, *Connectography: Mapping the Future of Global Civilization*, (New York: Random House, 2016), p.331.

3 Jun Osawa, "The Reversion of Cyberspace to the World of Classical Realism," *Japan SPOTLIGHT* (May/June 2018), pp. 22–24.

4 Anthony J. S. Craig and Brandon Valeriano, "Realism and Cyber Conflict: Security in the Digital Age," in Davide Orsi, J. R. Avgustin, and Max Nurnus eds., *Realism in Practice: An Appraisal* (Bristol: E-International Relations, 2018), pp. 85–101. However, while military power is emphasized as a constituent factor of power in classical realism, that characteristic does not apply in cyberspace.

5 Motohiro Tsuchiya, "Saiba supesu no gabanansu" [Governance of cyberspace], in *Gurobaru komonzu ni okeru nichibei domei no atarashii kadai* [Rising challenges for the Japan-U.S. alliance in the global commons], analysis report under the Japan Institute of International Affairs' fiscal 2013 investigation and research project on diplomacy and security for the Ministry of Foreign Affairs (March 2014).

could not interfere.

Subsequently, Richard Barbrook noted that the development of the Internet and its culture have a temporal and geographical bias. He stressed that the Internet was created on the west coast of the US during the 1960s, and this bias is characterized by "the Californian ideology" of optimism toward the future, belief in the ability to solve problems using technology, and the counterculture.[6] This geographical and temporal background made cyberspace "utopian." In cyberspace, there were to be no national boundaries, the state would be relativized, and hence there would be no international disputes. Even if there were cybercrimes, technology would resolve all the issues.

In addition, the expansion of cyberspace was in line with the trend toward globalization following the end of the Cold War. In the "flattened world" depicted by Thomas Friedman, not only enterprises but also individuals participate in global competition, and the state is relativized. Many of the factors that cause this flattening—including telecommunications technologies, general-use office software, and remote access—are related to the expansion of cyberspace.[7]

2. The "Hype" regarding Cyberspace and International Politics

However, the viewpoint of cyberspace as a "utopia" must be said to have been based on a lack of understanding and exaggerated premises regarding cyberspace and international politics: that is, it was based on "hype."

(1) Are there no boundaries in cyberspace?

The first "hype" is that there are no national boundaries in cyberspace. It is certainly true that digital information flies back and forth across national boundaries. Companies disperse their data centers all over the world, and users can utilize cloud services from anywhere on earth. The victims of cyberattacks, the servers that send attack orders, the transit points, the actual origins of the attacks, and the nationalities of the attackers all transcend national boundaries.

Nevertheless, each nation claims sovereignty and territoriality in cyberspace (or parts thereof), and in fact the "flow" and "stock" of digital information is being restrained by national boundaries.

As for the "flow," the fragmentation and Balkanization of the Internet is advancing. This is also called the "splinternet" in the sense that the original single Internet has become split.

China's Golden Shield Internet information censorship and blocking system constitutes a cyber Great Wall rising between the domestic Chinese and global Internets. Internet users have utilized the encryption technology of Virtual Private Networks (VPNs) to avert censorship and blocking by the authorities, but regulations on the use of VPNs have been reinforced since 2017. In May 2019, legislation was passed which makes it possible to cut off the Internet in Russia (Runet) from overseas. The Russian government asserts that this legislation is to protect the Runet from overseas cyberattacks and otherwise secure its continuity.

According to the report "Freedom on the Net" published by the US think tank Freedom House, a growing number of countries are imposing restrictions on user access and contents. Eric Schmidt, director of Alphabet, the holding company for Google has expressed concerns that if such regulations advance, then the global Internet may be transformed into a connected series

---

6 Richard Barbrook and Andy Cameron, "The Californian Ideology," *Science as Culture*, Vol. 6, No. 1 (January 1996), pp. 44–72.

7 Thomas Friedman, *Furattoka suru sekai: Keizai no daitenkan to ningen no mirai*, trans. Iwan Fushimi (Nihon Keizai Shimbunsha, 2006). Originally published as *The World is Flat: A Brief History of the Twenty-First Century*.

of nation-state networks.[8]

The regulation of "stock," that is, of where information will be stored, is also clear. According to one survey, countries are prohibiting the transfer of financial and settlement data, personal data, communications data, corporate confidential information, and various other data outside of their borders.[9]

This issue is not a simple structure of opposition between liberalism and authoritarianism (as discussed below). The Europe Union and Brazil, for example, prohibit the transfer of personal data outside their territories in order to protect privacy. China, Vietnam, and other countries require foreign enterprises conducting business in their countries to locate servers that store communications data, logs (records), and other important confidential information domestically, mostly for security, law enforcement, and the promotion of domestic industry. While the purposes for obstructing data transfer vary from country to country, this trend is referred to as "data localization."

Why can the state exercise sovereignty and territoriality in cyberspace (or parts thereof)? This is because cyberspace depends on physical infrastructure, and most physical infrastructure depends on territory and territorial seas. Digital information is stored on servers and at data centers, which exist within the soil of some country (recently, it is also being considered to locate data centers in territorial seas). More than 99% of international telecommunications on the Internet is via undersea cables which connect to land at the coastline of each country. Undersea cables themselves are laid on the seabed in international waters and are frequently jointly owned by companies in multiple countries, but their landing points and terrestrial sections at least lie within the territory of one country or another.

These observations are by no means new. Already in 2006, Jack Goldsmith and Tim Wu argued it is an illusion that cyberspace has no national boundaries, and noted that the state's mandatory power functions in cyberspace.[10] The fact that cyberspace depends on physical infrastructure is the basis whereby states exert (or can exert) sovereignty and territoriality in cyberspace; cyberspace fragmentation and data localization are the results of the exercise of state power.

(2) Is the power of the sovereign state relativized in cyberspace?

The second "hype" is that the power of the sovereign state is relativized in cyberspace. The state's monopoly on information and technology is destroyed, with individuals, enterprises, criminals, and terrorists all gaining power. Joseph Nye calls this development the "diffusion of power." He argues that the asymmetry of power between states and non-state actors is shrinking from the advance of technology.[11]

The combined sales of Google, Amazon, Facebook, and Apple (GAFA) total more than ¥70 trillion, surpassing the annual tax revenues of Japan, which is the world's third largest economy.[12] It is private-sector enterprises that operate the Internet and cyberspace.

---

8 Eric Schmidt and Jared Cohen, *Daigo no kenryoku: Google ni wa mieteiru mirai*, trans. Yuko Sakurai (Diamond-sha, 2014), p.129. Originally published as *The New Digital Age: Reshaping the Future of People, Nations and Business*.

9 Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" The Information Technology and Innovation Foundation (May 2017).

10 Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford: Oxford University Press, 2006). Wu is famous for coining the term "network neutrality."

11 Joseph S. Nye, Jr., *Cyber Power*, Belfer Center for Science and International Affairs, Harvard University (May 2010).

12 "Bocho GAFA: Kokka ga gyakushu (bundan no sakini)" [Expanded GAFA: State counterattacks (after the division)], *Nihon Keizai Shimbun* (March 10, 2019).

Cyberattacks are not the exclusive purview of nation states: they can be carried out by criminals, terrorists, and ultimately by individuals. By using encrypted messaging applications such as *Signal* and the encrypted network technology *Tor*, telecommunications contents and connection routes can be concealed, averting government surveillance (or so it is believed).

However, it is sovereign states which hold the most refined cyber capabilities, and looking back over the past 10 years, states were involved in most of the cyberattacks that had the greatest impact. It is highly likely that there was state involvement in Stuxnet (2010) which destroyed centrifuges at Iranian nuclear facilities, wide-ranging power outages in Ukraine (2015, 2016), interference in the US presidential election (2016), and the global spread of the ransomware WannaCry and NotPetya (2017), as well as the cyberattacks and big data collection that targeted the Japan Pension Service (2015),[13] the US Office of Personnel Management (2015), a leading US hotel chain (2018), and the Singapore government's medical database (2018).

Richard Bejtlich, who worked as the chief security officer at the US cybersecurity company Mandiant, notes that signal intelligence (SIGINT) capabilities are "one of the differentiators between nation state groups and other hacking units" in cyberspace. SIGINT capabilities that can intercept a large volume of Internet communications are an asset held only by nation states.[14]

Law enforcement is also a feature held only by the state. Under the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Washington can access data held by enterprises across national boundaries, and under the Cybersecurity Law, Beijing can access information stored on servers inside mainland China. GAFA and other enterprises "stock" massive data, but the sovereign state has superiority from the standpoint of "access" to data.[15]

While the asymmetry of power between states and non-state actors in cyberspace is certainly narrowing, the superiority of the sovereign state in sophisticated and continuous cyberattacks, data access, and other fields should not be overlooked.

(3) Does the expansion and deepening of cyberspace decrease international conflicts?

The third "hype" is that the expansion and deepening of cyberspace reduces international disputes. There are a few arguments regarding this point. One is that information technology itself will analyze social dynamics and the causes of disputes, predict the escalation of violence, and be helpful at times in conflict resolution and peace building. In a discussion with UN Assistant Secretary-General for Peacekeeping Operations Jane Holl Lute, Vint Cerf, who is recognized as one of the fathers of the Internet, suggested the potential contribution of technology because insight into the origins of conflicts is essential for conflict resolution.[16]

Another argument is that the expansion and deepening of cyberspace and the spread of the Internet in particular will promote the democratization of society and that if the number of democratic states increases, then wars will decrease. While this paper does not address the pros

---

[13] Although the government of Japan has not attributed the attacker in the Japan Pension Service case, according to the Macnica Networks report, it's obvious that the source of the attack was somewhere inside China. Macnica Networks, *Hyoteki gata kogeki no jittai to taisaku apurochi: Nihon wo osotta daikibo na saiba supai katsudo no jittai chosa* [Advanced Persistent Threat: A Survey of Large-Scale Cyber Spy Activities against Japan], 1st ed. (June 2016).

[14] Richard Bejtlich (@taosecurity), tweets at 00:50, October 5, 2018.

[15] However, there is also the opinion that big-tech companies have superiority in "access" as well. For example, the US government probably does not have a full grasp of what types of data are being collected and stored by enterprises and where the data are located. Without that information, the data cannot be accessed. This was noted by Koichiro Komiyama of the Japan Computer Emergency Response Team Coordination Center (May 7, 2019).

[16] Laura Ralston, "Can the Internet Solve Conflict?" *The World Bank Blog* (August 10, 2014); "Entrepreneurs Hunt for 'Peace Tech' to Defuse Conflict," *United States Institute of Peace* (September 24, 2014).

and cons of the democratic peace theory, even if one hypothetically accepts that wars do not break out among democratic states, it is questionable that the spread of the Internet advances democratization.

The Internet and other technologies do not always resolve conflicts and do not necessarily democratize society. That is because technologies are value neutral. In areas that seek freedom and democracy, they become tools for their pursuit, but authoritarian governments use the Internet and other information technologies as means for social control.[17] China's facial recognition and tracking technologies which it uses domestically and exports to European and other countries and its Social Credit System are typical examples. The Internet and related information technologies can be used as means of conflict resolution, but they can also be used to incite conflict and for mobilization, as demonstrated by the use of websites and social media by the "Islamic State" extreme terrorist organization to instigate terrorism in foreign countries and recruit "foreign fighters." How the expansion and deepening of cyberspace reduces international disputes is merely one aspect of the technology.

3. Great Power Competition in Cyberspace

Today, sovereignty and territoriality are being claimed even in cyberspace, and sovereign states are maintaining superior power in that realm. The expansion and deepening of cyberspace is not necessarily decreasing international conflicts, and is actually sparking new disputes in some cases.

(1) The US-China dispute regarding 5G and trade secrets

The US and China are presently in conflicts regarding cybersecurity issues. Specifically, these are the issue of excluding Chinese enterprises from the construction and operation of the fifth generation mobile telecommunications system (5G)—which is characterized by high speed and large capacity, low latency, and multi-connectivity—and the issue of the theft of trade secrets, intellectual property, and other assets of private enterprises via cyberattacks, etc. The US position is that the problems are (1) the Chinese government is collecting confidential information via Chinese enterprises, and (2) the Chinese government is engaged in cyberattacks targeting US private-sector enterprises. Moreover, the targets of cyberattacks by the Chinese government to steal confidential information overlap with China's "strategic emerging industries" (12th Five-Year Plan) and "10 key industries" (Made in China 2025).[18]

In 2018, the Donald Trump administration began to criticize Beijing, claiming that China was conducting ongoing cyberattacks on US private-sector enterprises. On October 4, Vice President Mike Pence criticized Beijing from start to finish in a nearly hour-long speech at the Hudson Institute. In addition to cyberattacks, Pence's speech covered a wide range of topics including election meddling, religious oppression, land reclamation in the South China Sea, and overseas investment that lacks transparency.

Throughout 2018, US authorities filed charges against officers of China's Ministry of State Security (MSS) and regional organizations under the MSS, the hacking group "APT10" which is linked to the MSS, and other Chinese enterprises and entities one after another for stealing trade secrets and intellectual property from US enterprises.

On January 28, 2019, the US Department of Justice announced charges against Huawei Device and its US subsidiary. The two firms were suspected of stealing trade secrets related to

[17] Ian Bremmer, "Democracy in Cyberspace: What Information Technology Can and Cannot Do," *Foreign Affairs*, Vol. 89, No. 6 (November/December 2010), pp. 86–92.

[18] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, February 2013; *Operation Cloud Hopper: Exposing a Systematic Hacking Operation with an Unprecedented Web of Global Victims*, PwC & BAE Systems (April 2017).

the quality testing robot Tappy owned by T-Mobile US, which is the US subsidiary of a leading German telecommunications firm. On that same day, in a separate case, the Department of Justice announced charges related to sanctions on Iran against Huawei Technologies, its Chief Financial Officer and Deputy Chairwoman Meng Wanzhou, Huawei Device's US subsidiary, and Skycom Tech.

But what gave an even greater shock than Pence's speech or the criminal charges was the National Defense Authorization Act for Fiscal Year 2019, which was passed into law with President Trump's signature on August 13, 2018. Section 889 of this Act excluded specified Chinese enterprises. Specifically, it excluded from US government procurement (1) specified Chinese telecommunications equipment manufacturers, (2) finished products assembled from components manufactured by these companies, and (3) companies using products manufactured by these companies. The five Chinese companies specified were Huawei Technologies, ZTE, the world's largest surveillance camera manufacturer Hangzhou Hikvision Digital Technology, the leading facial recognition technology manufacturer Dahua Technology, and the leading mobile radio systems firm Hytera Communications. With the exclusion of these enterprises from US government procurement, many corporations will be forced to greatly revise their supply chains.

Furthermore, Washington expanded the powers of the Committee on Foreign Investment in the United States (CFIUS) to review and regulate the foreign investments in the US more broadly than in the past.

Beijing criticized these responses by Washington as baseless. At the Mobile World Congress held in Barcelona in February 2019, Huawei Technologies Rotating CEO Guo Ping criticized the US. Borrowing from the famous lines about the magical mirror in the fairy tale *Snow White*, Guo said, "Prism, prism on the wall, who is the most trustworthy of them all? It is a very important question and if you don't answer that, you can go and ask Edward Snowden." PRISM is a surveillance program operated by the US National Security Agency (NSA) that was disclosed illegally by Snowden whereby NSA employees can search and collect metadata (data pertaining to data) from the Web mail and other services of US Internet companies.

The conflict between the US and China in 5G construction and procurement is deeply rooted. The National Intelligence Law of the People's Republic of China (in effect from June 28, 2017)—which stipulates in Article 7 that any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law, and keep the secrets of the national intelligence work known to the public[19]—is believed to be one reason for the concerns held by Washington and its allies regarding Beijing. Vice President Pence's speech at the Munich Security Conference (February 16, 2019) explicitly and the Australian government's decision on 5G procurement policy (August 23, 2018) implicitly showed deep concerns regarding Beijing's access to confidential information via Chinese enterprises.

However, it is overly simplistic to say that Washington's response changed because of China's National Intelligence Law. Information theft by Chinese entities is not a problem that suddenly arose after the start of the Trump administration. There was bipartisan support in the US Congress for making a strong response to Beijing and the alarm had already been sounded back in 2012.[20]

The US-China cybersecurity problem which emerged from 2013 is the background to the

---

[19] Shigako Okamura, "Chugoku no kokka joho ho" [National Intelligence Law of China], *Gaikoku no rippo* [Foreign legislation], no. 274 (December 2017), pp. 64–75.

[20] The October 8, 2012 report by the US House of Representatives Permanent Select Committee on Intelligence warns that the equipment provided by Huawei Technologies and ZTE poses a national security risk to the US, and that the US government should not use equipment from either of these companies.

exclusion of Chinese enterprises over 5G.[21] This issue is that a government steals trade secrets and intellectual property from foreign private companies for the purpose of gaining commercial advantages. In September 2015, Presidents Barack Obama and Xi Jinping agreed "that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[22]

Thereafter, however, cyberattacks from China targeting US enterprises did not decline. From the US side, this remains an unresolved issue despite the September 2015 agreement, that is, despite the commitment expressed by President Xi.

(2) The US-Russia dispute regarding elections and democracy

A dispute in cyberspace has also emerged between Washington and Moscow. US-Russian relations had grown tense over the Ukraine crisis (2014–), the Russian intervention in Syria (2015), the use of a Novichok nerve agent in the UK (2018), and other issues, but these were conflicts that occurred in American allies or third countries. It was the Russian interference in the 2016 US presidential election that directly harmed present US-Russian relations and occurred on American soil.

The Russian interference in the 2016 US presidential election can be broadly divided into three methods: (1) the theft and strategic disclosure of confidential information regarding candidates and political parties via cyberspace, (2) the distribution of false information and political advertising on social media and other channels, and (3) disruptive cyberattacks on voting and other election infrastructure.[23] Incidentally, suspicions of collusion between the Russian government and the Trump camp were not confirmed in the investigative report by special counsel Robert Mueller (March 2019).

The report (declassified version) by the Office of the Director of National Intelligence (ODNI) stated, "We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential 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" based on classified information and open source information.[24] Furthermore, the governments of the UK, Australia, the Netherlands, and Canada all concluded that the Russian government was responsible for the cyberattacks against Clinton's campaign and the Democratic National Committee (DNC) in 2016.

---

[21] For details, see Takahisa Kawaguchi, "Saiba sekyuriti wo meguru beichu tairitsu: Chiseigaku risuku ni kigyo wa do taiji subekika" [US-China confrontation over cybersecurity: How should enterprises handle geopolitical risk?], *Risuku manejimento today* [Risk management today], no. 113 (March 2019), pp. 4–8.

[22] The White House, Office of the Press Secretary, "FACT SHEET: President Xi Jinping's State Visit to the United States" (September 25, 2015).

[23] For details, see Takahisa Kawaguchi and Motohiro Tsuchiya, *Gendai no senkyo kainyu to nihon deno sonae: Saiba kogeki to SNS jo no eikyo kosaku ga kaeru senkyo kainyu* [Contemporary election interference and our preparedness in Japan: The impact of cyber attacks and influence operations on social networks], Tokio Marine & Nichido Risk Consulting (January 28, 2019), appendixes 1 and 2, http://www.tokiorisk.co.jp/service/politics/rispr/pdf/pdf-rispr-01.pdf.

[24] "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution," Office of the Director of National Intelligence (January 6, 2017), p. ii.

Thereafter, three indictments[25] charged the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), its cyber espionage group Fancy Bear (also known as APT28), the Internet Research Agency (IRA), which is a company located in Saint Petersburg, and other organizations and individuals, and they were subjected to economic sanctions by the US Department of the Treasury.

Among the acts of interference in the 2016 US presidential election, the Obama administration was aware of the cyberattacks on Democratic Party organs and election infrastructure from a relatively early stage during the presidential campaign. However, the awareness of the threat of the distribution of political propaganda and disinformation via Russian media outlets (RT, Sputnik, etc.) and via social media during the campaign was insufficient.[26]

As Facebook, Twitter, and other social media came to be recognized as venues for electoral activities and consensus formation, intentional obstruction and manipulation of elections on social media and other platforms by foreign governments were positioned as a national security issue. This situation is named "LikeWar" by P. W. Singer.[27] What Russia hacked was not only Democratic Party organs and election infrastructure but also the sentiment and voting behavior of the American citizen, and ultimately their democracy.

Following the 2016 US presidential election, interference by foreign governments was confirmed in the November 2018 US mid-term elections as well. The US intelligence community investigated interference in the mid-term elections based on Executive Order 13848. They concluded that while they were unable to confirm "any compromise of our nation's election infrastructure that would have prevented voting, changed vote counts, or disrupted the ability to tally votes," they did confirm that "Russia, and other foreign countries, including China and Iran, conducted influence activities and messaging campaigns."[28] These influence operations are becoming the "new normal."

(3) US-Europe confrontation

The axes of confrontation in cyberspace run not only between the open liberal societies and closed autocratic societies. While the US and European countries fundamentally share the same standpoints regarding cybersecurity, they are in confrontation in several fields. Alec Ross, who served as the principal Internet policy advisor for the Department of State in the Obama administration, said that while "the great struggles of the 20th century were between left and right, the conflict of the 21st century will be between open and closed."[29] The US and Europe are in conflict with different positions on "open" and "closed," depending on the field.

---

25 U.S. District Court for Eastern District of Virginia, *Indictment*, Case 1:18-MJ-464 (September 28, 2018); U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00032-DLF (February 16, 2018); U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00215-ABJ (July 13, 2018).

26 For example, while election interference by Russia was first publicly mentioned at the October 7, 2016 joint press conference by Director of National Intelligence James Clapper and Secretary of Homeland Security Jeh Johnson, this only referred to cyberattacks on the Democratic Party organs and election infrastructure. For details, see Kawaguchi and Tsuchiya, *Op. Cit.*, appendixes.

27 P. W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York: Eamon Dolan / Houghton Mifflin Harcourt, 2018).

28 Office of the Director of National Intelligence, "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" (December 21, 2018).

29 Will Englund, "Russia hears an argument for Web freedom," *The Washington Post* (October 28, 2011). However, what Ross had in mind was the opposition between open societies such as in Europe and the US and the closed societies of China, Russia, etc.

The US and Europe, and Japan as well, are in agreement that the existing international law applies in cyberspace. They have confirmed that stance at the United Nations Group of Governmental Experts (GGE) and at the Group of Seven (G7) leading industrialized nations, and in bilateral and multilateral agreements.

However, the US and Europe have clear differences regarding the regulation of personal data. In light of the collection of vast amounts of personal data by Facebook, Google, and other platform companies and the surveillance programs whose existence was revealed illegally by Edward Snowden, the EU General Data Protection Regulation (GDPR) entered into force in May 2018. In this regard, it would be appropriate to say that the EU, which prohibits the transfer of personal data to outside the region in principle, is "closed," while the US, which has no such restriction, is "open."[30]

What is more, the US has warned its European allies that it will no longer be able to share classified information with them if they allow Huawei Technologies to participate in their 5G procurement activities. Regarding this issue of excluding Chinese enterprises from 5G, while the US has designated specific Chinese companies, the UK's policy is apparently that the risk can be acceptable and managed even if Chinese firms participate. More precisely, the UK seems to consider that because the security of 5G cannot be ensured by excluding certain companies, a combination of various methods such as monitoring and countermeasures is effective. Here, we can see an axis of opposition between a "closed" US and an "open" Europe.

Of course, "open" does not always mean "good." In national security and other fields, there are cases where "closed" is appropriate.

Conclusion

There was a time when the appearance of cyberspace centered on the Internet, and the expansion and deepening of cyberspace, were expected to greatly change the established system of sovereign states. However, cyberspace proved to be no great exception to the existing sovereign state system from the perspectives of national boundaries, asymmetry of power, and international disputes in cyberspace. The emerging disputes between major powers are disputes regarding the theft of confidential information in cyberspace and interference in elections via cyberspace: they are problems arising from the expansion and deepening of cyberspace.

"State-centrism" is expanding in cyberspace in the sense that sovereign states exercise power centered on their national security, and there are cases where disputes and confrontations between major powers are occurring.

[30] But the state of California, where many US information technology companies are located, passed the California Consumer Privacy Act of 2018, which takes effect from January 2020. Moreover, there are frequent discussions regarding a comprehensive privacy bill at the federal law level.