Digital Space – Beyond Internet

Kilnam Chon

Contents

(1) Introduction

The Internet turned fifty-years old in 2019, with more than half of the global population as its users [Internet 2020]. There are various application systems based on digital technologies with the Internet and other networks as their infrastructure. We refer to these application systems as aspects of digital space. The aspects include artificial intelligence, data, social media, cybersecurity, and Internet of things (IoT) among others. Digital space and cyberspace have drawn a great deal of attention in this century, with various conferences and organizations devoted to them [Cyber 2013; Seoul 2013; ECIR 2013; Black 2010; Cyberspace 2013; Chon 2013b]. This article explores 'digital space' (and cyberspace), and its subspaces; digital economy and digital society. We also explore aspects of the digital space. We will then explore governance of digital space and its aspects. This article also comments on the relationship between digital space and COVID-19 in the appendix.

In this paper, we use "cyberspace" and "digital space" interchangeably except for cases where it is necessary to separate them. Wikipedia defines cyberspace as "a concept describing a widespread, interconnected digital technology"[Wikipedia 2020]. This definition could also be used for digital space. Other similar terms such as digital world, cyber world, virtual space, and virtual world can be considered as well. Cyberspace has been discussed since the mid-1990s when the word was coined by several people including William Gibson. The word cyberspace was given prominence in his book Neuromancer [Gibson 1984]. "Digital" was elaborated by many people including Nicholas Negroponte. He wrote the book, Being Digital in 1995 [Negroponte 1995]. Digital space is a more neutral term than cyberspace. The cyberspace tends to be understood in the context of cybersecurity or cyberwarfare. Digital space is more harmonized with digital economy and digital society than cyberspace, too. Cyberspace tends to imply cyberwarfare, especially in the USA and Europe. In 2010, the US White House issued a report entitled "International Strategy for Cyberspace" [White House 2012]. The US government designated a 'Cyber Command' as the fifth domain after land,

sea, air, and space. The European Union as well as the UK government followed suit by forming similar organizations. These initiatives brought worldwide attention to the ideas of cyberspace as well as cyber warfare.

(2) Digital Space

Digital Space, Real Space, and Mixed Space

Digital space is a virtual space that is typically based on the Internet whereas real space is based on the physical world we live in. Additionally, there is mixed space consisting of both digital space and real space. Figure 1 shows a representation of these spaces,

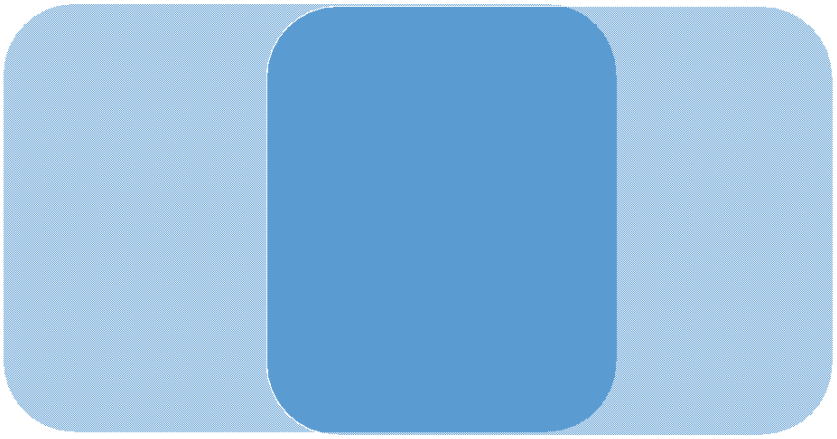

Figure 1 Digital Space, Mixed Space, and Real Space

Some mixed spaces are called cyber-physical systems, such as a sensor-based network system where the Internet and other networks are used. Many Internet-based systems tend to be mixed spaces rather than pure digital spaces without any real space component.

Digital Space and the Internet

Digital space, when referring to digital society and digital economy, has the Internet as its infrastructure in most cases. But some digital spaces have other network infrastructures – for example, a telephone system without the Internet, a television system without the Internet, or a sensor-based network system [Claffy 2013]. Digital space has various aspects including cybersecurity, artificial intelligence, data, social media and Internet of things (IoT) among others. See Figure 2 for a diagrammatic representation of digital space, its subspaces, its aspects, and infrastructure.

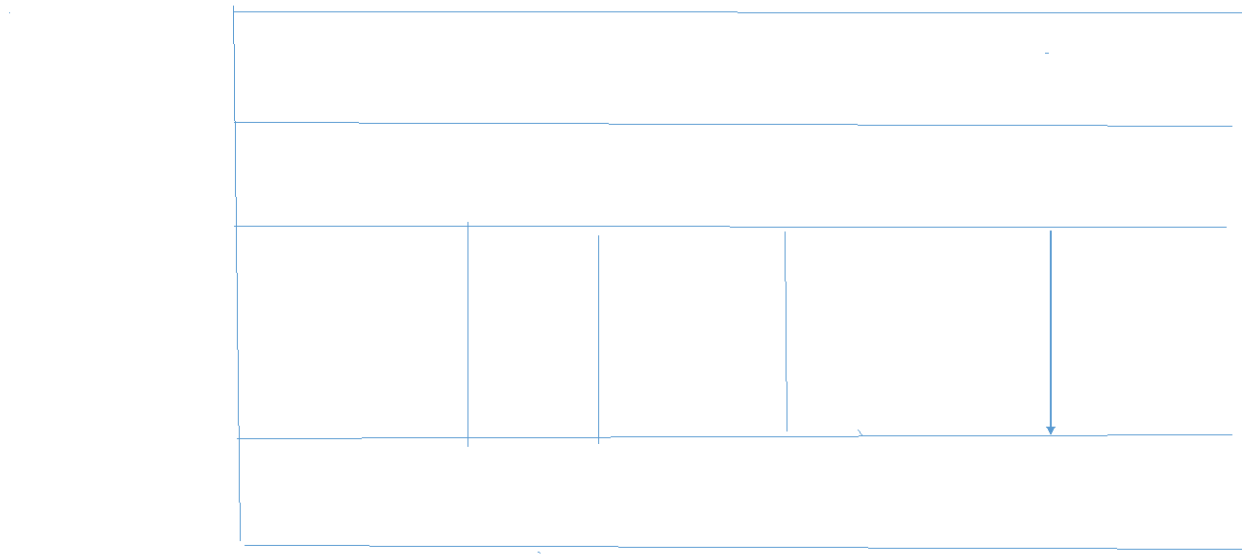

Figure 2 Digital space, Subspace, aspects and infrastructure

(3) Subspaces of Digital Space; Digital Economy and Digital Society

David Clark, in his paper "Three Views of Cyberspace", emphasized three facets [Clark 2011]:

Cybersecurity
Cyber Economics
Cyber Society

Anthony Giddens, in his paper "Four Dimensions of Globalization", proposed four dimensions of globalization to which Gabriela Tejada added culture as the fifth dimension [Tejada 2007, Giddens 1991]:

World Capitalist Economy
Nation-State System
World Military Order
(International) Division of Labor
Culture

Kilnam Chon proposed the following major aspects in his paper [Chon 2013]:

Cyber Society
Cybersecurity
Cyber Economy
Cyber Nation-State

Cyber Environment

Additional aspects such as Digital Education, and Digital Labor may also be considered as aspects of digital space according to Kilnam Chon.

Digital Society

Digital society, including digital culture, is closest in meaning to 'the Internet' as they cover a similar semantic domain. With this understanding, digital society governance would be similar to Internet governance [IGF 2020]. Both digital society governance and Internet governance cover multiple social issues such as privacy, security, abuse, addiction, and violence, among others. The concepts of digital society and digital culture cover a range of contents, but the term 'the Internet' tends to cover this same range in a more partial fashion. The Web Index by the Web Foundation may be the only index that covers various aspects of digital society as well as digital economy, as many indexes on digital space tend to consider only the digital economy [Web 2012].

Digital Economy

Digital economy is one of two subspaces of the digital space that has been developed extensively in this century. UNCTAD's Digital Economy Report 2019 stated:

"In 2016, the Digital Economy represented $11.5 trillion, or 15.5 percent of global GDP – 18.4 percent of GDP in developed economies and 10 per cent in developing economies, on average. It found that the digital economy had grown two and a half times faster than global GDP over the previous 15 years, almost doubling in size since 2000."

There are other indexes on the digital economy including Internet Matters by McKinsey, and the Network Readiness Index by the World Economic Forum [UNCTD 2019; McKinsey 2012; World 2019; Boston 2011].

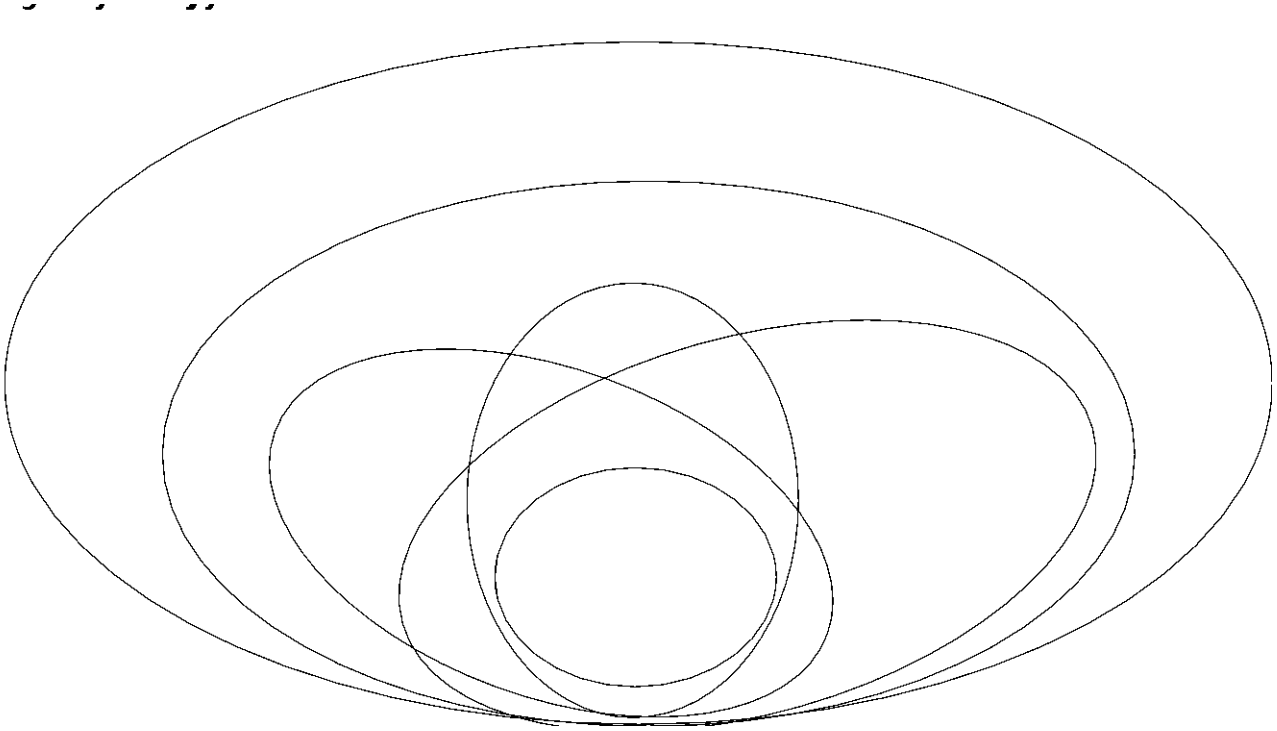

Figure 3 Digital Economy and Other Economies

(4) Aspects of Digital Space

There are five aspects of digital space which we have identified so far.

Artificial Intelligence (AI)
Data
Internet of Things (IoT)
Cybersecurity
Social Media

These aspects are covered at Asia Pacific School on Internet Governance (APSIG) in its annual schools in 2010s [APSIG 2020]. Governances of these aspects are also covered in the APSIG annual schools.

In this chapter, we will cover these five aspects. Other aspects may be covered later. This would require much efforts. We would like to see a "complete" set of the aspects sometime in future.

Artificial Intelligence (AI)

Artificial intelligence (AI) with the Internet and other technologies had the major development in this century [Lee 2018; Chon 2018b; McKinsey 2018; PwC 2017; Stanford

2015; Russell 2019]. Most of the current AI development is closely coupled with the Internet along with big data and high performance computing which is typically based on cloud computing as well as AI algorithms. Kai-Fu Lee calls this development the first wave of AI, which is taking place in the first decades of the twentieth century.

Almost all major companies working on AI are also major companies on the Internet. They include Amazon, Apple, Facebook, Google and Microsoft in the USA, and Alibaba, Tencent, and Baidu in China. We expect the symbiotic relationship between AI and the Internet to be kept for a long time to come.

Consulting companies such as McKinsey and PwC are forecasting AI's contribution to the global economy as around $15 to 20 trillion in 2030 [McKinsey 2018; PwC 2017]. This is roughly 15-20% of the global economy. AI is expected to impact almost every aspect of the economy and society in the coming years. AI governance is an important issue for the digital society, too, and will be described in the next chapter along governances of other aspects.

Data

Data, in particular big data, also has a symbiotic relationship with the Internet. We had one zettabyte in 2009. The growth of data in the digital space was 33 zettabytes in 2018 and is expected to be 175 zettabytes in 2025 with an exponential growth curve in the foreseeable future [IDC 2018]. The big data is also a necessary component of AI growth. Handling of these data raises many issues including privacy, ownership of the data, and abuse of the data among others. Data governance in the next chapter explores on these issues including General Data Protection Regulation (GDPR), which was developed in the EU recently [Park 2018; EU 2016].

Internet of Things (IoT)

Internet of Things (IoT) is developed to serve devices rather than people through the Internet. IoT development started in the last century, and grew substantially in this century and surpassed the human users in this decade [Chon 2017; Kondepudi 2015]. We expect the number of devices to be connected to the Internet to grow from around 10 billion in 2015 to 100 billion or more in the next decade. We also had Mirai, the first case of malware through IoT, in 2016. IoT governance including IoT security and standardization are now important issues [IETF 2019; Kondepudi 2015].

Cybersecurity

Cybersecurity has been one of the most visible aspects of digital space in this decade, partly due to the addition in 2011 of the cyber domain to the four previously recognized domains – land, sea, air, and (outer) space – in the military conceptualization by the USA, EU, and UK governments. Specifically, the organizations charged with preparing for cybersecurity and cyber warfare are as follows:

USA: Cyber Command (USCYBERCOM)
EU: European Network and Information Security Agency (ENISA)
UK: Government Communications Headquarters

Many conferences on cybersecurity were held during 2010s. Some worthy of mention include the following:

International Conference on Cyberspace
Cyber Dialogue
ECIR Workshops
FIRST Conference
Global Cyberspace Cooperation Summit

The Stuxnet incident in 2011 as well as the cyber attack on Estonia changed the cybersecurity landscape by bringing the concepts of cyber warfare and cyber weaponry into currency [Sanger 2012, Clarke 2010].

Cooperation on cybersecurity incident responses have been coordinated nationally, regionally and internationally with establishment of organizations after the first worm, called Morris Worm in 1988 [Wikipedia 2020]. They started with Computer Emergency Response Team Coordination Center (CERT/CC) in 1988 and Forum of Incident Response and Security Team in 1990 [Wikipedia 2020b; Wikipedia 2020c]. Please refer Chapter 5 Cybersecurity of Asia Internet History, Third Decade (2000s) on these organizations. Please also refer APSIG on its classes on cybersecurity APSIG 2020].

Social Media

Social media is another important aspect in this century. Please refer Chapter 3 Social Media of Asia Internet History, Third Decade (2000s) for detail description. People tend to access social media for interacting in the digital space rather than the traditional Internet applications. Notable social networking service websites include Facebook, Twitter, Instagram, Weibo, and LinkedIn. Messaging services are also very popular, and they include WhatsApp, Facebook Message, WeChat, Line, and Kakao Talk. Social media is replacing the traditional Internet applications, particularly in East Asia where the messaging service and e-commerce are dominant applications now. Please also refer Section 3.5 Social Media Governance of Asia Internet History, Fourth Decade (2010s) for additional information.

Other Candidate Aspects

Digital Nation State may cover legal systems for digital space as well as the international relations in digital space, which may be substantially different from those of real space. Explorations on Cyber International Relations (ECIR) covers the cyber nation state extensively – in particular, the facet of international relations [ECIR 2012]. The International Conference on Cyberspace also covers the international relations aspect of the cyber nation state [Cyber 2011].

Digital Environment is a new aspect that needs to be studied thoroughly. The digital environment on its own is very important including both the (sustainable) digital environment itself, as well as the requirements of the cyber environment needed to support a sustainable

physical environment [Chon 2012]. While we work on a sustainable digital environment, we also need to work on mixed environments that consist of digital and physical environments including cyber-physical systems.

Names and Numbers are managed by Internet and other organizations globally. IP addresses in both their IPv4 and IPv6 formats as well as other numbers including the Autonomous System Number are managed by the Number Resource Organization (NRO) with the close cooperation of the Internet Assigned Numbers Authority (IANA) of the Internet Corporation on Assigned Names and Numbers (ICANN) now. Media Access and Control (MAC) address is a unique identifier assigned to a network interface for communications. It is typically used with Ethernet with MAC address allocation being handled by IEEE through its 802 Committee. Domain names are managed by ICANN including Top Level Domain Names (TLDs) in English alphabets and other characters. International Organization for Standardization (ISO) handles the standardization of information technology including country codes, which are used for the domain name and others.

Some of the following areas may be considered as digital space aspects, too.

Digital Education
Digital Labor
Digital Health

(5) Global Standards

Global standards for digital space are handled by various organizations with the close collaboration of national, regional and global standards bodies, which include the following:

- Institute of Electrical and Electronics Engineers (IEEE)
IEEE is a technical professional organization for advancement of technology. IEEE Standard Association works on industry standards
through 802 Committee and the related registration authority on MAC address.

- Internet Engineering Task Force (IETF)
IETF is the standards body for Internet protocols, and it was founded in 1986, taking over the work of the Network Working
Group of the ARPANET Project begun in the late 1960s. This includes Request for Comments (RFC), the Internet standard
documents.

- International Organization for Standardization (ISO)
ISO handles variety of standards including information processing. Many of them are relevant to Digital Space.

- International Telecommunication Union (ITU)
ITU handles standardization and allocation on telecommunication including spectrum allocation [Restrepo 2019].

- World Wide Web Consortium (W3C)
W3C is the standards body for WWW-related technologies such as HTML and HTTP.

- The 3rd Generation Partnership Project (3GPP)
The 3GPP is a collaboration among the telecommunications associations of the USA, Europe, China, Japan, and South Korea
to develop standards for the third-generation mobile phone system and next generation mobile phone systems.

(6) Governance of Digital Space and Its Aspects

The Working Group on Internet Governance (WGIG) of the United Nations defined Internet governance as follows [WGIG 2005]:

> "*Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.*"

The Internet governance principles was revised at NETmundial Meeting in 2014 [NETmundial 2014].

For digital space, we may look into broadening the concept of the governance now. Many aspects of digital space are in their early stages, and their governance may be substantially different from the Internet governance. The concept of the governance in the Internet governance may not work well as we are discovering in cybersecurity governance and artificial intelligence governance. The ECIR workshop on "Who controls cyberspace?" is of great interest since we still do not know how digital space will be controlled or governed [ECIR 2012].

Some aspects of the digital space governance may be appropriate to consider now. On the other hand, cybersecurity governance may be premature, which is somewhat similar to the state of nuclear technology governance in the 1950s [Nye 2011]. We may eventually need cybersecurity governance in a similar way to nuclear technology governance, which requires treaties and inspection protocols.

IGF Workshop on "Cyberspace Governance – Exploration," was held in 2013 to discuss digital governance [Chon 2013b]. Asia Pacific School on Internet Governance offered classes on governances of various aspects in 2016-2019 including Data Governance, IoT Governance, Cybesecurity Governance, AI Governance, and Social Media Governance [APSIG 2020].

Artificial Intelligence Governance

Artificial intelligence governance has finally attracted much attention globally with various conferences and meetings, and various publications [Chon 2019; Russell 2019; FLI 2017]. AI governance may be substantially different from Internet governance in many ways. First of all, we are unable to develop any consensus on the AI principles, and we have many versions

of the AI principles at present. We may also need regulations by governments since human safety is at stake such as autonomous driving. AI was included in the existential risk list issued at Cambridge University and others. Industry is playing a major role in AI governance in this century, too.

Data Governance

Data governance is closely related to AI governance as well as privacy governance [Park 2017]. The European Union (EU) came up with General Data Regulation Policy (GDPR) in 2016, which was accepted by many countries and regions in addition to Europe [EU 2016]. We expect GDPR to take a lead on the data governance development in the coming years.

IoT Governance

IoT governance may be developed similarly to the Internet governance, and we may consider the IoT governance as a subset of the Internet governance [Chon 2017]. The differences in these two governances may include standardization and users. The IoT standards are mostly developed by industry consortia rather than global non-profit organizations such as IETF [Kondepudi 2015]. The number of "users" in IoT exceeded human users of the Internet in this decade already, and we expect to have more than 100 billion devices connected to the Internet in the coming years and decades.

Cybersecurity Governance

Cybersecurity governance has been addressed actively in this decade [Tikk 2018; Chon 2016; Komiyama 2019; Cyberspace 2011]. There was much effort on developing the global norm on cybersecurity through UN and other organizations, but a consensus among governments has not been developed. It may take much effort and time before we come up with a good cybersecurity governance model for the world. Meantime, there is reasonably good governance on the operational level through national and regional computer security incident response teams (CSIRT) with the global organization called FIRST, regional organizations on all regions, and national organizations in addition to other organizations in each country [Wikipedia 2020b; Wikipedia 2020c].

Social Media Governance

Social media governance is attracting much attention lately [Park 2019]. We are having many important issues on the social media including misinformation, abuse, and ownership on social media data among others. The social media governance is becoming closely related to the AI governance now. This makes the social media governance much more complex.

Other Governances

Governance of other aspects such as privacy and other human rights issues as well as social issues such as education and work may need to be addressed. The governances on these aspects may take much different formats than the governance of other aspects, and they would be the major challenges in the coming years and decades.

(7) Issues

Global forums on governance of digital space, its aspects, and subspaces

A few global forums currently exist that deal with digital space, including the following:
RightsCon
Internet Governance Forum

RightsCon covers almost all areas of digital space with its over twenty program categories [RightsCon 2019]. Internet Governance Forum also covers many areas with four tracks; data, environment, inclusion and trust in its 2020 meeting[IGF 2020]. The global forums on digital space are still in their infancy as all of them were founded recently or their coverages have been expanded to cover digital space. We need to look into what we need in this area globally, regionally, and nationally.

Aspects

The aspects listed in this article were developed with the bottom-up approach, i.e., exploring aspects which have been attracting attention lately. How can we come up with the "complete set" of the aspects so that we could cover the digital space comprehensively? The digital space could then be the digital world to complement the real world. Please refer articles by Joseph Nye, David Clark, Kilnam Chon, and Anthony Giddens among others on their opinions on the aspects [Nye 2014; Clark 2011; Tejada 2007; Chon 2013].

Subspaces

Are two subspaces prosed in this article; digital economy and digital society appropriate? Do we need more subspace or do we need a different set of subspaces?

Globalization vs Fragmentation

The digital space is being globalized including aspects and subspaces as well as its infrastructure; the Internet and the telecommunication networks. We may be facing fragmentation of the digital space as well as the Internet in the coming decades [Drake 2016].

(8) Concluding Remarks

The digital space, including its various aspects, is still in its early conceptual stages, as explained in this paper. We examined definitions of digital space along its subspace: the digital society and the digital economy. Then, we explored five aspects of the digital space. We would like to see further studies on the digital space, the subspaces, and its aspects as well as their governances in the coming years.

The digital space is being developed at a rapid pace in this century. AI, big data, and IoT are playing major roles in the development of the digital space now. All of the trillion-dollar companies are from the digital space now. For example, the market capitalization of all automobile companies amounts to less than the market capitalization one of the largest digital space companies. These trends would continue in the coming decades. The current coronavirus-19 (COVID-19) crisis is also contributing to its development.

We wrote the article, "Cyberspace – What is it?" and organized the workshop, "Cyberspace

– Exploration" in 2013. This article, "Digital Space – Beyond Internet", is a major revision of the 2013 article. We had two "once in a century" developments, artificial intelligence and COVID-19, in this decade. We would like to revisit the digital space within the coming decade to find out if we have to go through another major revision on the digital space.

References

[AAAI 2018] AAAI and ACM, AI, Ethics and Society Summit, Honolulu, 2018.

[Almeida2016] Virgilio Almeida, Cyberspace Governance, Harvard University, 2016.

[APSIG 2020] Asia Pacific School on Internet Governance, APSIG.asia, 2020.

[Asia 2020] Asia Internet History Project, Third Decade (2000s), 2020.

[Attali 2008] Jacques Attali, After the Crisis, 2008.

[Baig 2020] Aamer Baig, et al., The COVID-19 recovery will be digital: a plan for the first 90 days, Mckinsey, 2020.

[Black 2010] Black Hat Computer Security Conference, July 2010.

[Bell 2020] We need mass surveillance to fight COVID-19, but it needs not have to be creepy, MIT Tech Review, 2020.

[Bonvanie 2017] Rene Bonvanie, Sharing of data, algorithm, Global Cyberspace Summit, 2017.3.17.

[Boson 2011] Boston Consulting Group, e-Intensity, 2011.

[Brooks 2020] Joseph Brooks, An extraordinary period in internet history: Akamai data shows 30% surge in internet traffic, 2020.

[Cerf 2020] Vint Cerf, Internet lessons from COVIT19, COVID19 and Internet Openness, 2020.5.14.

[Choi 2019] Yang Hee Choi, Future of ICT, Computer History Workshop, Jeju, 2019.

[CE 2011] Council of Europe, The (Budapest) Convention on Cyber Crime, 2011.

[Chon 2012] Kilnam Chon, Ecological Internet, NORDUNET, 2012.

[Chon 2013] Kilnam Chon, Cyberspace – "What is it?", Cyber Commons. 2013.

[Chon 2013b] Kilnam Chon, et al., Workshop on Cyberspace Governance – Exploration, IGF, Bali, October 2013.

[Chon 2013c] Kilnam Chon, Cyberspace – "What is it?", 2013.

[Chon2014] Kilnam Chon, Cyberspace Governance, 2014.

[Chon2016] Kilnam Chon, Cybersecurity Governance, 2016.

[Chon2017] Kilnam Chon, IoT Governance, 2017.

[Chon2018] Kilnam Chon, Digital Governance, 2018.

[Chon 2018b] Kilnam Chon, AI: Past and Present, 2018.

[Chon2019] Kilnam Chon, AI Governance, 2019.

[Chon2019b] Kilnam Chon, Internet Governance and AI Governance, 2019.

[Chon 2019c] Kilnam Chon, Internet Governance History, 2019.

[Chon 2020] Kilnam Chon, Digital Space - Introduction, 2020.

[Chon 2020b] Kilnam Chon, Coronavirus and Internet, 2020.

[Choucri 2012] Nazli Choucri, Cyberpolitics in International Relations, MIT Press, 2012d.

[CFR 2018] Council of Foreign Relations, "What is the digital society we want to build together?", 2018.

[Claffy 2013] KC Claffy and David Clark, Platform Models for Sustainable Internet Regulation, TPRC 41, 2013.

[Clark 2011] David Clark, Three Views of Cyberspace, ECIR, Harvard-MIT, 2011.

[Clarke 2010] Richard Clarke, Cyber War, 2010.

[CyberCommons 2012] CyberCommons.net, 2012.

[CyberDialogue 2013] Cyber Dialogue Conference, 2013.

[Cyberspace 2011] Global Conference on Cyberspace, 2011.

[Dafoe2018] Allan Dafoe, AI Governance: Research Agenda, Oxford University, 2018.

[Dafoe2019] Allan Dafoe, AI, Strategy, Policy and Governance, Beneficial AI, 2019.

[DocFilm 2019] DocFilm, Omnipotent Amazon, DW, 2019.05.11.

[Drake 2016] William Drake, et al., Internet Fragmentation – Overview, World Economic Forum, 2016.

[EastWest 2015] East West Institute, Promoting international cyber norms, 2015.

[Economist 2010] Cyberwar, Economist, 2010.7.1.

[ECIR 2012] ECIR Workshop: "Who Controls Cyberspace?", 2012.

[ECIR 2013] Explorations in Cyber International Relations, ECIR.MIT.edu.

[ESCAP 2020] ESCAP/APCICIT, How Korea turned tide on COVIT-19 using ICT, 2020.4.28.

[EU 2016] EU, General Data Protection Regulation (GDPR), 2016.

[FIRST 2020]

[FLI 2017] Future of Life Institute (FLI), Asilomar AI Principles, 2017.

[Gibson 1984] William Gibson, Neuromancer, Ace Books, 1984.

[Grey 2020] John Grey, Why this crisis is a turning point in history, New Statesman, 2020.3.

[Heaven 2020] Will Heaven, Why the coronavirus lockdown is making the internet stronger than ever, MIT Tech Review, 2020.

[ICANN 2020] ICANN, ICANN's Early Days, ICANN History Project, 2020.

[IDC 2018] IDC, Data Age 2025: Digitization of the World, 2018.

[IEEE 2015] IEEE, IoT Ecosystem Study – Executive Summary, 2015.

[IETF 2019] IETF, Internet of Things (IoT) Security, RFC 8576, 2019.

[Internet 2020] Internet World Stats, 2020.

[IGF 2020] Internet Governance Forum.

[Komiyama2019] Koichiro Komiyama, Cybersecurity Governance, APSIG, 2019.

[Kondepudi 2015] Sekhar Kondepudi, IoT Standard War, Forum on IoT, ITU, 2015.

[Korea 2020] Korean Government, Flattening the curve on COVID-19, UNDP, 2020.4.16.

[Larik 2015] Joris Larik, Cyber Governance: challenges, solutions and lessons for effective global governance, 2015.

[Liaropoulos 2016] A. Liaropoulos, Exploring the complexity of digital space governance, J. of Information Warfare, 2016.

[McKenzie 2011] Alex McKenzie, INWG and the conception of the Internet: An eyewitness account, IEEE Annals of the History of Computing, Vol 33, No1, 2011.

[McKinsey 2011] McKinsey, Internet matters, 2011.

[McKinsey 2018] McKenzie, Promise and challenge of the age of AI, 2018.

[McKinsey 2020] McKenzie, COVID-19 recovery will be digital: A plan for the first 90 days, 2020.5.14.

[Munich 2011] Munich Cybersecurity Conference, 2011.

[Netmundial 2014] Netmundial, 2014.

[Negroponte 1995] Nicholas Negroponte, Being Digital, 1995.

[Nye 2011] Nuclear lessons for cybersecurity, 2011.

[Nye 2014] Joseph Nye, Regime complex for managing global cyber activities, GCIG, 2014.

[OECD 2017] OECD, Digital Economy Outlook, 2017.

[Park2018] KS Park, Data Governance, APSIG, 2018.

[Park 2019] KS Park, Social Media Governance, APSIG, 2019.

[Park 2020] KS Park, Social Media Governance, 2020.

[Park 2020b] KS Park, Data Governance, 2020.

[PwC 2017] PwC, Global Artificial Intelligence Study: Sizing the Prize, 2017.

[Restrepo 2019] Joaquin Restrepo, Spectrum allocation for 5G international framework, ITU, 2019.

[Russell 2019] Stuart Russell, Human Compatible, 2019.

[Sanger 2012] David Sanger, Confront and Conceal, 2012.

[Security 2018] Security Today, Cyber Ecosystem, 2018.
[Stanford 2015] Stanford University, Stanford AI 100 Report, 2015.

[Stevens 2018] Tim Stevens, Cyberweapons: Power and governance of the invisible, Journal of International Politics, 2018.

[Seoul 2013] International Conference on Cyberspace, Seoul, 2013.

[Taparin 2020] Hans Taparin, Future of college is online, and its cheaper, New York Times, 2020.

[Tejada 2007] Gabriela Tejada, The four dimensions of globalization according to Anthony Giddens, GLOPP, 2007.

[Tikk 2018] Eneken Tikk, Cybersecurity Governance, APSIG, 2018.

[UN 2015] UN GGE Report, Major players recommending norms of behavior, 2015.

[UNCTD 2019] UNCTAD, Digital Economy Report 2019.

[UNDP 2020] UNDP Flattening the curve on COVID-19, 2020.4.16.

[Web 2012] Web Foundation, Web Index.

[Web 2017] Web Foundation, White Paper on AI: Road ahead in low and middle-income countries.

[WGIG 2005] Working Group on Internet Governance, WGIG Report, 2005.

[White House 2011] Whitehouse, International Strategy for Digital space, 2011.

[WGIG 2005] Working Group on Internet Governance (WGIG), Final Report, 2005.

[Wikipedia 2020] Wikipedia, Morris Worm, 2020]

[Wikipedia 2020b] Wikipedia, CERT, 2020.

[Wikipedia 2020c] Wikipedia, FIRST, 2020]

[WSIS 2005] World Summit on Information Society (WSIS), Tunis Agenda, 2005.

[World 2019] World Economic Forum, Network Readiness Index, 2019.

[Worldometers 2020] Worldometers.info, 2020.

[Wu 2003] Tim Wu, Net Neutrality, 2003.

[Zuboff 2019] Shoshana Zuboff, The age of surveillance capitalism, 2019.

Appendix Coronavirus and Digital Space

Coronavirus 19 (or SARS-CoV-2, or COVID-19) is taking over the world since it was announced as pandemic by the World Health Organization in March 2020. There are a total confirmed infection cases of 4,721,828 and total confirmed deaths of 313,260 affecting 213 countries and territories as of 2020.05.17 [Worldometers 2020]. This pandemic is an extraordinary case in modern human history.

John Grey wrote an article, “Why this crisis is a turning point in history” in 2020 with the following quote [Grey 2020];

“….There will be celebrations as the pandemic recedes, but there may be no clear point when the threat of infection is over. Many people may migrate to online environments like those in Second Life, a virtual world where people meet, trade and interact in bodies and worlds of their choosing…..”

Brian Chen wrote the following in the New York Times on 2020.4.15:

“A computer with a good internet connection, communication apps and entertainment are the only tech we really need, ever.”

Many people around the world really live in the digital space much of time lately due to the COVID-19 pandemic. A recent study indicated a 30% sudden increase of Internet traffic in East Asia according to Akamai [Brooks 2020]. Many could not go out for work, school, and so on due to nation-wide lockdowns. Moreover, they are afraid of infection by meeting people physically, but feel comfortable to meet them in the digital space with computers, smartphones, television, and other audio-visual equipment since they offer non-contact meetings.

In many countries with lockdowns, regular K12 education as well as college education is now being done in the digital space rather than the physical world. Online education used to be a complementary tool. This is no longer the case [Taparin 2020]. Much of daily work is also done in the digital space rather than by commuting to offices. Much of shopping is similarly done in the digital space through e-commerce. This sudden change is due to the risk of infection in the real world through physical contacts.

The digital space with the current reasonable matured technologies is providing a very important alternative now. But it also has drawbacks, however, including the following.

- Handicapped people, physically or economically have a similar or worse handicap in digital space.
- Governments tend to use digital space technologies for surveillance and other privacy infringement to fight against the pandemic, and may not give up these technologies when the pandemic is over.

What will happen to the world after this pandemic is over? We may not be able to go back to the pre-COVID-19 world, and the digital space of the post-COVID-19 will be different from the digital space of the pre-COVID-19 [McKinsey 2020]. We need to carefully look into issues on the digital space and the mixed space for the post-COVID-19 world.