CYBERSPACE ETHICS: FINDING AN EQUILIBRIUM BETWEEN FREEDOM AND PROTECTIONISM

Haekal Al ASYARI[*]
Muhammad Ardiansyah ARIFIN[**]
Yosephine GRACE[***]

Abstract

Cyber freedom refers to an approach at regulating cyberspace that opposes state monopoly over cyberspace regulatory making. A compelling argument for this concept could be argued by the nature of the most known cyberspace instrument: the internet. According to Lessig, the internet was designed for research, not the concealment of information. In the meantime, many states believe that limiting the cyberspace is a way forward. By exercising jurisdiction to constituting cyberspace facilities, data governance, and cyber operations, the sovereign will be able to protect cyberspace from harm and unnecessary chaos. Practically put, states are divisive in adopting between favouring a multi-stakeholder approach and a government centred authority. Despite owing the nature of cyberspace to be borderless and limitless, human beings are still the inherent subject and bearer of responsibility and liability of every conduct in cyberspace. Human naturally possess values of norms and ethics. As the creator and centrepiece of every activity in the virtual world, cyberspace is built on the foundations of ethics. The priority to serve basic human needs, respect for privacy and freedom, equality, and inclusivity, as well as to protect and not destroy are the four-fundamental ethics of cyberspace. This article attempts to validate the existence of those ethics, despite the different normative approaches each state may adopt. To that end, it also suggests an innocent proposal to how the freedom of cyberspace may be limited, and how the protectionist is able to unshackle restrictions to position cyberspace on a purposive scale for every human need.

Keywords: *cyberspace, ethics, equilibrium freedom, protection.*

1. Introduction

Cyberspace has been a point of interest in the digital age because of its utility. According to Stückelberger, cyberspace is a whole virtual reality space that is parallel and has uncountable interactions with the physical world[1]. Muhamad Rizal and Yanyan M. Yani stated that cyberspace is a new world brought by the internet—beyond computer systems—which enables various people to connect with anyone and anywhere[2]; widening the sope of cyberspace. According to Dysson, there are five characteristics of cyberspace: (1) it

[*] Ph.D. candidate, "Marton Géza" Doctoral School of Legal Studies, University of Debrecen, Hungary (e-mail: haekal.al.asyari@ugm.ac.id).

[**] Undergraduate student, Faculty of Law, Universitas "Gadjah Mada", Yogyakarta, Indonesia (e-mail: muhammadardiansyah00@mail.ugm.ac.id).

[***] Undergraduate student, Faculty of Law, Universitas "Gadjah Mada", Yogyakarta, Indonesia.

[1] Stuckelberger Christoph and Duggal Pavan, *Cyber Ethics 4.0: Serving Humanity with Values*, ed. Ignace Haaz and Samuel Davies (Geneva: Globethics.net, 2018), 23.

[2] Muhamad Rizal and Yanyan Yani, *Cybersecurity Policy and Its Implementation in Indonesia, JAS (Journal of ASEAN Studies)* 4, no. 1 (August 2016): 61, https://doi.org/10.21512/jas.v4i1.967.

operates virtually; (2) it is rapidly dynamic; (3) borderless and not limited to territorial boundaries; (4) it enables people to be anonymous; (5) it contains public information.[3]

In cyberspace, people around the world interact in various activities. These people are often called 'netizens' which means citizens of the internet.[4] Netizens are individuals who use the internet for different purposes and collectively it connotes the citizen of the internet.[5] As a jargon, 'netizen' means professional use of the internet for meritorious motives.[6] Generally, netizens' various use of the internet includes using electronic mail, online chatting, instant messaging, internet forums, blogging, commenting in various platforms, file sharing, information creating, surfing, and others.[7] The activities done by netizens include them to be a part of the cyber society, due to the link and influence that it has on every individual.[8]

Unfortunately, activities in cyberspace do not conform with cyber ethics. Cyber ethics is a field of applied ethics which examine moral, legal, and social issues in the use and development of cyber technology. Cyber ethics does not only focus on good practices that are safe and polite in cyberspace, but also concerns itself with moral, legal, and social issues related to computers and the internet as a platform for human interaction.[9] Indonesian netizens 'protested' the removal of Indonesian badminton team by filling the All England Instagram account with inflammatory comments in the new posts—and the All England changed their Instagram account not long after.[10] This was one of the contemporary cases of unethical practices by netizens in Indonesia. A similar 'online ambush' reoccurred in February 2021 to Microsoft because Microsoft published a report which placed Indonesian citizens as one of the most impolite netizens in South East Asia.[11] More general and global examples include unsolicited e-mail advertising and spam,[12] cyberbullying,[13] and other unethical behaviour such as fantasy of illegality in the virtual world and virtual theft.[14]

[3] Ahmad Rudy Fardiyan, Etika Siber Dan Signifikansi Moral Dunia Maya, in *Prosiding Seminar Nasional Komunikasi: Akselerasi Pembangunan Masyarakat Lokal Melalui Komunikasi Dan Teknologi Informasi.* (Lampung: Universitas Lampung, 2016), p. 334.

[4] Michael Seese, *Scrappy Information Security*, ed. Kimberly Wiefling (Silicon Valley: Happy About, 2009), p. 130.

[5] Femi Richard Omotoyinbo, *Online Radicalisation: The Net or the Netizen?*, *Social Technologies* 4, no. 1 (2014), pp. 51-61, https://doi.org/10.13165/ST-14-4-1-04.

[6] Omotoyinbo, p. 54.

[7] Chai Lee Goi, *Cyberculture: Impacts on Netizen*, Asian Culture and History 1, no. 2 (July 1, 2009), p.141, https://doi.org/10.5539/ach.v1n2p140.

[8] Stuckelberger Christoph and Duggal Pavan, *Cyber Ethics 4.0: Serving Humanity with Values*, ed. Ignace Haaz and Samuel Davies (Geneva: Globethics.net, 2018), p. 15.

[9] Fardiyan, *Etika Siber Dan Signifikansi Moral Dunia Maya*, p. 334.

[10] M. Hafidz Imaduddin, *Akun Instagram 'Baru' All England Langsung Diserbu Netizen Indonesia*, Kompas, 2021, https://www.kompas.com/badminton/read/2021/03/20/15491538/akun-instagram-baru-all-england-langsung-diserbu-netizen-indonesia?page=all.

[11] CNN Indonesia, *Sebut Netizen RI Paling Tidak Sopan Akun Microsoft Diserang*, CNN Indonesia (Jakarta, 2021), https://www.cnnindonesia.com/teknologi/20210226140821-192-611309/sebut-netizen-ri-paling-tidak-sopan-akun-microsoft-diserang.

[12] Alfreda Dudley et al., *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices*, ed. Lindsay Johnston Kristin Klinger Erika Carter, Myla Harty, and Sean Woznicki, 1st ed. (Hershey: IGI Global, 2012).

[13] Dudley et al., p. 69.

[14] Dudley et al., pp.118-119.

Law and morality are two normative systems that has been regulating and controlling powers over the behaviours of individuals, aiming to maintain a harmonious state between individuals who recognize each other's rights. Additionally, both systems, although in some ways very different, have a complementary relationship in which morality lessens the rigid implementation of positive law and law compensates for the weaknesses of morality in its functions and implementation.[15] Concurrently, law has an ongoing impact on morality, vice versa, since morality is historically contingent and law is an influential factor in the contention on morality.[16] Morality and ethics are linked together, although both are somewhat different. Ethics, ideally, is a code of law that prescribes the correct behaviour universally, one that differentiates between good and evil,[17] and are governed by experts and professionals (external factors) while morality transcends through cultural norms and are governed by oneself. Moreover, ethics can have no morals and one could violate ethical principles to maintain one's moral integrity. Consequently, there should be a main goal on the implementation of ethics with morals in the world of cyberspace through laws.

With the aforementioned characteristics of cyberspace, it can be confirmed that it inherits multilingual, multicultural, multireligious, and multilateral components of individuals belonging to different nationalities.[18] Thus, ethics in cyberspace is global, interconnected, multicultural, multireligious and multiphilosophical. Despite such diversity, common grounds are found by extracting values from the sources of different countries and international organizations.[19] The international community, through the United Nations, have agreed upon that all cyber related activities have to be measured against the benchmark of Sustainable Development Goals (SDGs).[20] Some of the thresholds include that cyberspace has to prioritize to serve basic human needs; respect privacy and freedom; increase equality and inclusivity; as well as protect and not destroy life.[21] The manifestation of these values are centred upon the perception that the purpose of technology is to serve human beings. In this context, it is inarguable that human—as the prime regulatory body—has full control in guiding how we exist in cyberspace. The link between rule of ethics for visions, orientations, and community, and rule of law for reliability, trust, and control of power ought to be implemented in every regulating sector from education, commerce, health care, and security. An initial question then appears: how does ethics guide the legal framework of cyberspace?

When observing the legal framework for cyberspace, a division is made between cyber liberalism and cyber protectionism.

[15] Willy Moka-Mubelo, *Law and Morality*, in Reconciling Law and Morality in Human Rights Discourse: Beyond the Habermasian Account of Human Rights, vol. 3 (Cham: Springer International Publishing, 2017), pp. 51–88, https://doi.org/10.1007/978-3-319-49496-8_3.

[16] George P. Fletcher, *Law and Morality: A Kantian Perspective*, Columbia Law Review 87, no. 3 (April 1987), pp. 533-558, https://doi.org/10.2307/1122670.

[17] Zygmunt Bauman, *Morality without Ethics*, *Theory, Culture & Society* 11, no. 4 (November 29, 1994), pp. 1–34, https://doi.org/10.1177/026327694011004001.

[18] Christoph and Pavan, *Cyber Ethics 4.0: Serving Humanity with Values*, p.16.

[19] Ibidem.

[20] International Telecommunication Union, *ICTs for a Sustainable World #ICT4SDG*, International Telecommunication Union, 2021, https://www.itu.int/en/sustainable-world/Pages/default.aspx.

[21] International Telecommunication Union.

With the prior opts for complete freedom and unlimited use and exploitation of cyberspace, while the latter prefers the suppression of such freedoms. Cyber protectionism is a broad term that refers to a wide range of barriers to digital trade (e-commerce) and cross-border data flows,[22] with examples such as censorship, filtering, localization measures and regulations to protect privacy.[23] Meanwhile, cyber liberalism, also known as cyber freedom mainly comprises the right to internet access, freedom of expression and information, and freedom from internet censorship. The relevance of these concepts stem from its different manifestation in regulations. The different types of regulation will determine different user behaviours reacting to the limits of their activities. These regulations, however, take off from a positivist orientation, which often leaves out crucial philosophical basis of such norms. Here, the need for cyber ethics presence itself. By determining the fundamental ethics of cyberspace, a threshold for liberalizing and limiting the breadth of user activities through regulation is hoped to be accommodated.

Ethics are dependent on oneself, although it is relatively consistent within a certain context, it still varies from one person to another considering that every human being has their own ethical standards. Therefore, ethics can be deemed as borderless. In cyberspace, a borderless virtual reality that is parallel with the physical world,[24] law and morality should always be inherent and applied by society. This concept is derived from the maxim "ubi societas, ibi ius" which means, wherever there is society, there is law. Thus, wherever there's society, there is law and there are ethics. All three are co-dependent with each other in both physical and virtual worlds. Furthermore, after researching the concerning condition of cyberspace this paper aims to straighten out and deepen the research on ethics, moral, and law of cyberspace, specifically on cyber ethics and cyber law, finding the equilibrium between cyber freedom and cyber protectionism. In doing so, the analysis of this research is limited to the scope of examining cyber ethics that are manifested in regulations and how it may affect user activities in cyberspace. The issue of cybercrime will not be extensively discussed, as opposed to the normative governance of international and national framework of a few countries such as the United States and China.

Herein, two literary works are referenced. The first in regards with cyber ethics fundamentals that has been presented by Christoph Stückelberger and Pavan Duggal.[25] Out of the 25 chapters that are discussed in their work, the novelty that this article brings is the discussion of cyber ethics between the freedom of cyberspace and protectionism. The second is referred to Andrew Power and Gráinne Kirwan where their discussion of ethics and legal aspects of virtual worlds gives extensive highlights on cybercrime and legal enforcement.[26] This will not be considered since the issue of enforcement and criminal law is humbly reserved for future discussion.

This research applies a philosophical-normative approach, which mainly analyses

[22] Susan Ariel Aaronson, *What Are We Talking about When We Talk about Digital Protectionism?*, World Trade Review 18, no. 4 (August 6, 2019), pp. 541-577, https://doi.org/10.1017/S1474745618000198.

[23] United States International Trade Commission, *Digital Trade in the U.S. and Global Economies*, Part 1, 2013, p. 21.

[24] Christoph and Pavan, *Cyber Ethics 4.0: Serving Humanity with Values*, p. 23.

[25] *Idem*, p.16.

[26] Dudley et al., *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices*, pp.117-131.

the background and core values to cyberspace in relation to relevant legal framework of different states. This paper primarily assesses international law, national law, as well as literature relating to ethics, cyberspace, and cyber governance. The analysis is elaborated through a qualitative method on how ethics, in the context of cyberspace acts as pillars and foundations of the legal framework for governance and regulations both internationally and nationally. Two main legal perspectives will be analysed; from countries that adopts a more liberal orientation towards cyberspace, and its protectionist counterpart. From this comparative analysis, it is hoped to conclude that the essence of ethics is found in both approaches, despite the differences in its formulation into the relevant legal framework.

Thus, an urgency exists to create limits and regulations against the negative use of cyberspace that is built based on cyber ethics. Much like laws and regulations that apply in the real world, ethical principles that govern human acts and conduct should also need to be applied equally in cyberspace. By finding the balance between cyber freedom and cyber protectionism, cyber ethics will guide a rational value-driven legal framework, for individual's engagement for the fruitful use and presence of cyberspace.

2. Roots of Ethics in Cyberspace

The cyberspace is a borderless domain and was free from regulations and restrictions that epitomize the real world.[27] This statement would have been somewhat accurate if it was resented a few decades ago. Due to the immaculate progress and development, it has gone through, cyberspace is no longer free. where most of the credit is given to globalization and commercialization. In the sense that its intellectual commons are shared among states,[28] prevalent filtering,[29] increased awareness in privacy and anonymity,[30] and an active engagement for cyber sovereignty.[31] But has it always been this way? or has these boundaries been put in place and its exposure are delayed. One essence is of certain; ethics and moral values are inseparable from the cyberspace.[32]

In the era where information is an essential commodity, the inception of ethics prevents the cyberspace to be used in an ill-mannered way.[33] A normative regime for cyberspace must be equipped with values that are inherent to human. Thus, not only the absence of normative regime in cyberspace will allow malicious actors to

[27] Richard A Spinello, *Code and Moral Values in Cyberspace*, Ethics and Information Technology 3, no. 2 (2001), pp. 137–50, https://doi.org/10.1023/A:1011854211207.

[28] Jean Buttigieg, *The Common Heritage of Mankind From the Law of the Sea to the Human Genome and Cyberspace*, Symposia Melitensia 8, no. Special Issue (2012), pp. 81-92.

[29] UNGA, *United Nations General Assembly Resolution, The Right to Privacy in the Digital Age, UN Doc A/RES/68/167* (2014), UNHRC, *United Nations Human Rights Council Decision, Panel on the Right to Privacy in the Digital Age, A/HRC/DEC/25/117* (2014); UNHRC, *United Nations Human Rights Council Decision, The Right to Privacy in the Digital Age, A/HRC/28/L.27*, (2015).

[30] Joel Trachtman, *Cyberspace, Sovereignty, Jurisdiction, and Modernism*, Indiana Journal of Global Legal Studies 5, no. 2 (1998), pp. 561-581.

[31] Christoph and Pavan, *Cyber Ethics 4.0: Serving Humanity with Values*, p. 23.

[32] Nneka Obiamaka Umejiaku and Mercy Ifeyinwa Anyaegbu, *Legal Framework for the Enforcement of Cyber Law and Cyber Ethics in Nigeria*, International Journal of Computers & Technology 15, no. 10 (2016), pp. 7130-7139, https://doi.org/10.24297/ijct.v15i10.12.

[33] UNGA, *United Nations General Assembly Resolution, Combating the Criminal Misuse of Information Technologies, A/RES/55/63*, (2001).

operate in a grey area, but the chances of misuse are immeasurable if values are not embedded in such framework. But where did these ethical values come from? Was it created at the same time computers were invented? Or did it come at a later stage once human discovers the limitless that they can do on the internet?

If we look back to 1992, the Computer Ethics Institute came up with 10 commandments of computer ethics,[34] which include to not use computer to harm other people, interfere with others work, snoop, steal, or lie; to not use software illegally; to not use unauthorized computers, claim others' work, and to use computers in a respectful manner. This was a decade after the invention of the internet, when the use of cyberspace was still uncommon. But it is already observed that humans wanted to have the internet to be put to good use, despite knowing the possibilities of harm that it could also create. Clearly, a basic understanding of right and wrong had already been established.

Today, cyberspace has become a domain of its own. It consists of inter-connected networks, people from across nations, fusing cultures and languages from all ages and occupation supplying and demanding information which can be transmitted in a matter of seconds.[35] Despite this transformation, it is considered that the much-recognized ethics of today are re-inventions of the old.[36] The difference lies where some values have been incorporated into binding laws. This assumes that some ethics are still on the basis of self-responsibility and self-regulation within the conscious of individuals that exist in cyberspace. In differentiating one from another, Stùckelberg have divided it into fundamental premise, fundamental values, contextual values, and discretionary decisions.[37] This hierarchy is presented based on the binding character of norms, from the strongest to weakest respectively. Ethics that are manifested into laws, both national and international, are placed on the position of contextual values. Thus, it is bound by a context of particular space and time; and binding upon specific subjects.[38]

As a representation of collective goals and aspirations of the international community, the United Nations Sustainable Development Goals (SDGs) are indispensable from the roots of ethics.[39] A reason to why it is centered on human rights norms. For the goals of the SDGs to be realized by the member states, public trust and confidence is centered on the basis of ethics.[40] Within this context, it is to be understood that the cyberspace as the heart for the flow information, like any other essential commodity must also be governed by ethics. The four ethical values presented in the beginning of this paper were by means of Stückelberger and Duggal's generous analysis. Since 'to serve basic human needs' and 'protect and not destroy life' are obvious and broad elements, we have selected the remaining three: respect for privacy and freedom, equality, and inclusivity.

It is acknowledged that the UN SDGs, formalized through the General Assembly is of non-binding character, and thus absent

[34] Diane Bailey, *Cyber Ethics*, 1, New York: The Rosen Publishing Group, 2008, p. 10.
[35] Fuentes-Camacho Teresa, *Introduction: UNESCO and the Law of Cyberspace*, in The International Dimensions of Cyberspace Law, 2nd ed., Routledge, 2000, pp. 27-36.
[36] Christoph and Pavan, *Cyber Ethics 4.0: Serving Humanity with Values*, p. 36.
[37] *Idem*, p. 39.
[38] *Idem*, p. 40.
[39] Jerome Amir Singh, *Sustainable Development Goals: The Role of Ethics*, Sight Life 29 (2015), pp. 56-61.
[40] *Ibidem*.

from any compliance of accountability mechanism. The legal binding nature of such an instrument will not be the subject of debate within this paper. Because despite positioning the UN SDGs as a main source of contextual values, other treaties, customs, principles, and documents of international law have also reiterated similar values.

Classical human right treaties have represented a general consensus on the vitality for the right of privacy, and access to information.[41] Other set of regional agreements also reaffirms the right of everyone to hold opinions without interference, as well as the freedom of expression, to seek, receive, and impart information and ideals of any kind, rights concerning the respect for privacy.[42] On the outskirts of these values, it can be concluded that the threshold for the right to privacy and freedom must be on the balance between the interest of law enforcement and respect for fundamental human rights.[43]

As a common heritage of mankind,[44] cyberspace should be open and utilized for the benefit of every living individual and future generations. Equality and inclusivity of access must be guaranteed by every nation. Despite the flow of information might arguably be subject to sovereignty, a complete blockade from it should not. This value is emphasized numerous times during the General Assembly meetings. Member States have understood that the free flow and universal access to information goes hand in hand with global cyber security, protection of critical information structure, and the development of ICTs.[45] Unfortunately, the concept and manifestation between ethics and the law that have been presented is an expectation of the ideals. Despite cyberspace existing virtually as a single-integrated domain, individuals are still subject to the sovereignty and jurisdiction of every state. Having each sovereign varying from their legal system, culture, social structure, political and economic environment, cyberspace too is inevitably governed in a different way. The nature of this governance

[41] UNGA, *Universal Declaration of Human Rights*, United Nations, 1949, Articles 12 and 19; Council of Europe, *European Convention on Human Rights* (1950), Articles 8 and 10; UNGA, *International Covenant on Civil and Political Rights* (1966), Article 17.

[42] Organization of American States, *American Convention on Human Rights*" (1969), Article 11; League of Arab States, *Arab Charter on Human Rights* (2004), Articles 16 and 21; ASEAN Secretariat, *ASEAN Human Rights Declaration and Phnom Penh Statement on the Adoption of the ASEAN Human Rights Declaration* (Phnom Penh: Association of Southeast Asian Nations, 2012), Article 21; Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (European Treaty Series - No. 108)" (1981); Council of Europe, *Directive 2016/680 of the European Parliament and the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA*, Official Journal of the European Union § (2016).

[43] Council of Europe, *Budapest Convention on Cybercrime* (European Treaty Series - No. 185), (2001), pt. Preamble.

[44] Haekal Al Asyari, *Cyberspace as a Common Heritage of Makind: Governing Jurisdictional Limitations of the Internet by Virtue of International Law*, (University of Debrecen, 2020).

[45] UNGA, United Nations General Assembly Resolution, *Combating the criminal misuse of information technologies*, A/RES/55/63; UNGA, *United Nations General Assembly Resolution on the Creation of a Global Culture of Cyber Security, A/RES/57/239* (2003); UNGA, *United Nations General Assembly Resolution Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, A/RES/58/199* (2004); UNGA, *United Nations General Assembly Resolution on the Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures, A/RES/64/211* (2010), https://doi.org/10.1680/jdare.16.00049; International Telecommunication Union, *World Summit on the Information Society Outcome Documents, Geneva 2003 - Tunis 2005*, (Geneva; Tunis, 2005).

is split between one that prefers it to be free, and the other prioritizing its protection.

Declan McCullagh believes that the government is the enemy of cyberspaces vitality and openness.[46] In contrast, Lessig maintains that government policy will be needed as a corrective to private parties who seek to undermine the liberating technology; particularly those that are changing the internet's character. Spinello, who supported Lessig's claim, believes that the cyberspace will still attain its freedom if moderated and guided by government policy sensitive to human rights and freedom-enhancing values.[47] Our stance stands close to the later, freedom on the cyberspace has to be guaranteed by law; where such rules and regulations are inherent to fundamental ethics.

3. Freedom of cyberspace: a theoretical paradox?

The advancement of technology strongly influences the development of ethics. Technology was made, and is continually evolving, to ease human lives. However, it cannot be constituted as ethically 'neutral' since technology essentially shapes and reveals what humans value.[48] Technology continually reshapes the global distribution of power, justice, and responsibility; distributing both negative and positive impacts unevenly.[49] In order to ensure that the great benefits of technology and exposure to their risks are distributed properly, it entails the necessity of justice, which is fundamentally an issue of ethics.[50] In this case, the technology at hand is manifested in the form of cyberspace—the absence of it is closely linked to the normative framework.

More than fifty declarations, regulations, and guidelines were adopted in the last decades in regards to internet governance.[51] However, only one third of such documents show the necessity and importance of ethics in regards to the use of cyberspace.[52] The lack of governance on ethics proves on the absence of ethics in cyberspace first and foremost before even diving into relevant cases on such issue. Without ethics controlling and limiting the actions of users, cyberspace becomes the place chaos.

The main causes of the absence of ethics, that were already detected in the 1990s and are still relevant today, lie in the freedom in cyberspace. First, the freedom of access to information results in a vast amount of information being easily accessible and downloaded by individuals for their own interest such as copying, printings, scrutiny, and show.[53] Freedom of access to information also results to "information wants to be free" which causes the corrupted expectation of not being obligated to pay for information with its

[46] Spinello, *Code and Moral Values in Cyberspace*, p. 137.
[47] *Idem*, p. 139.
[48] William J Rewak and Shannon Vallor, *An Introduction to Cybersecurity Ethics* (Santa Clara: Santa Clara University, 2018), p. 3.
[49] Rewak and Vallor, p. 3.
[50] Rewak and Vallor, p. 4.
[51] Rolf H. Weber, *Ethics as Pillar of Internet Governance*, Jahrbuch Für Recht Und Ethik / Annual Review of Law and Ethics 23 (2015), p. 95.
[52] Rolf H Weber, *Principles for Governing the Internet: A Comparative Analysis*, Paris: UNESCO Publishing, 2015, p. 54.
[53] Roger Clarke, *Ethics and the Internet: The Cyberspace Behaviour of People, Communities and Organisations*, Business and Professional Ethics Journal 18, no. 3 & 4 (1999), p. 159, https://doi.org/10.5840/bpej1999183/423.

appropriate price. There is countless amount of book piracy committed online, enabling users all over the world to illegally download different kinds of books. Unfortunately, only one of many examples that constitutes as normal practice today that are not properly dealt with. The second lies the in the freedom to act anonymously, leading to uncontrollable actions.[54] Studies have suggested that anonymity can significantly increase aggression[55] and the likelihood of regulations being broken,[56] due to its nature of acting as a mask for the users. Anonymity prevents the identification of the culprit of any crime or misdemeanours, not able to hold them accountable. Particularly, freedom to access information and to act anonymously enhance some of the characteristics of cyberspace—operating virtually, its borderless nature and not limited to territorial boundaries, and the ability to be anonymous.[57] Hence, this research will further discuss on the vast and continuous effects of the freedoms, acting as a double edged sword in the realm of cyberspace.

Four integral issues have become apparent in the world of cyber ethics in which are free speech, intellectual property rights protection, privacy, and security.[58] These four issues emerge as cyberspace does not only become the tool for research and communication, but also for entertainment, commerce, and social media; creating and expanding more platforms, thus giving more space to commit various actions, both negative and positive. Consequently, with the absence of ethics, threats arising from those issues become blatant as their negative effects influence the cyberspace into becoming a place of negativity and unsafe territory.

Cyberspace lets individuals exercise the freedom of expression, enabling features for users to contribute to various platforms. Due to freedom of online expression, free speech branches out many different types of negative effects such as hate speech, harassment, bullying, spam, discrimination, pornography.[59] Those effects are evident in forms of racism, misogyny, sexism, and xenophobia—in which all are still blatant until today. 'Memes' are one of the modern examples that can embody the negative impacts of free speech,[60] where it is a very powerful tool that can go viral easily. Memes in most cases are harmless and have the purpose to entertain. However, if it contains negative and degrading content and with its nature of easily going viral, it can ruin the lives of people and/or institutions. Unfortunately, cases of free speech are hard to investigate, and perpetrators are often left unaccountable due to the nature of cyberspace, turning such fundamental right into a double-edged sword. Limitations of free speech are written in many laws and regulations both in national and international levels. However, due to the nature of

[54] *Ibidem.*

[55] Philip G Zimbardo, *The Human Choice: Individuation, Reason, and Order versus Deindividuation, Impulse, and Chaos*, in *Nebraska Symposium on Motivation*, University of Nebraska Press, 1969, pp. 237-249.

[56] M E Kabay, *Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy*, in Annual Conference of the European Institute for Computer Anti-Virus Research (EICAR) (Munich, 1998), pp. 1-40.

[57] Fardiyan, *Etika Siber Dan Signifikansi Moral Dunia Maya*, p. 334.

[58] Richard A. Spinello, *Ethics in Cyberspace: Freedom, Rights, and Cybersecurity*, in *Next-Generation Ethics*, Cambridge University Press, 2019, p. 446, https://doi.org/10.1017/9781108616188.029.

[59] Spinello, p. 447.

[60] Nicolle Lamerichs et al., *Elite Male Bodies: The Circulation of Alt-Right Memes and the Framing of Politicians on Social Media*, Journal of Audiences& Reception Studies 15, no. 1 (2018), pp. 1–27.

cyberspace, it becomes difficult and taxing to handle.

The notion "information wants be free" made by scholars goes against and at the same time redefines intellectual property protection law. Intellectual property rights protect the author's right of any scientific, artistic, or literary work, protecting their moral and economic rights. Unfortunately, intellectual property rights are hard to maintain in cyberspace, due to its nature and the absence of ethics. The borderless nature of cyberspace significantly increases the ability to make and distribute copies of music, books, and videos, resulting to violations of intellectual property law that are not seriously dealt with. Humans indeed have the right to access their basic need of information, but this becomes controversial in a way violating those who owns or obtained the intellectual property rights. Although some states heavily regulate intellectual property rights, handling cases of violations become tedious and difficult with the fast-moving and borderless nature of cyberspace.

Privacy in cyberspace is best described as a virtual space where individuals can be free from interruption or intrusion and where they can control the time and manner of the disclosure of their personal information.[61] Privacy is a fundamental human right. However, privacy in cyberspace is hard to maintain because every action always leaves a digital footprint. Digital technology becomes the driving force of the development privacy in which when cyberspace is included in the formula of processing of personal data, it shifts the notion to a new dimension that includes the notion of data protection.[62] Internet cookies, as one of the modern forms of data collection in cyberspace, are made to track, personalize, and save information about the users.[63] They are created to identify users and process their data based on their digital footprints, thus sparking threat against privacy when misused. Loose privacy enforcement regulations are also evident in how major technology companies like Facebook, Google, and Amazon constantly monetize the flow of information by turning them into profits.[64] Once again, due to the nature of cyberspace, maintaining privacy becomes strenuous and difficult, thus holding perpetrators of violations against privacy accountable becomes harder. The lack of ethics in its regulations further prove this notion.

Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption.[65] However, due to the open nature of cyberspace, users become vulnerable to cybersecurity threats. Cybersecurity threats aim to damage data, steal data, or obstruct digital life in general in the forms of data breaches, viruses, or cyber-attacks. Cybercrimes have increased by 600% during the pandemic and continue

[61] S. K. Verma and Raman Mittal, *Legal Dimensions of Cyberspace*, ed. S K Verma and Raman Mittal, New Delhi, Indian Law Institute, 2004, p. 451.

[62] Danilo Doneda and Virgilio A.F. Almeida, *Privacy Governance in Cyberspace*, IEEE Internet Computing 19, no. 3 (May 2015), p. 3, https://doi.org/10.1109/MIC.2015.66.

[63] Kaspersky, *What Is a Cookie? How It Works and Ways to Stay Safe*, Kaspersky, 2021, https://www.kaspersky.com/resource-center/definitions/cookies.

[64] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, *Defining Cybersecurity*, Technology Innovation Management Review 4, no. 10 (October 30, 2014), pp. 14-21, https://doi.org/10.22215/timreview/835.

[65] James A. Lewis, *Cybersecurity and Critical Infrastructure Protection*, Center for Strategic & International Studies, 2006.

to increase as years pass by,[66] growing at an unprecedented pace, making cybersecurity a prevalent issue. Various laws and regulations on cybersecurity have been made and implemented in numerous jurisdictions. However, those lack focus on ethics of its users.

The free regime of cyberspace–operating virtually and containing public information, is rapidly dynamic, borderless, and anonymous–offers many opportunities for its users. Four main sectors that are boosted by the free regime of cyberspace are the economy, information, and communication sectors. These four sectors have increased its quality and use at an unprecedented pace as cyberspace continues to evolve.

Cyberspace plays a critical role in the global economy, making economy rely greatly on cyberspace infrastructure and establishing digital revolution.[67] Cyberspace has affected the economy in three major interrelated ways.[68] First, cyberspace promotes equality and inclusion in a way that it lowers the cost of information and expands the market as a result—making a mutually beneficial transaction easier for everyone. E-commerce platforms gives opportunities to all business, from big to small, to find customers. Second, cyberspace has made vast number of efficient improvements in which transactions between sellers and customers are made cheaper, faster, and more convenient—raising productivity. Details of transactions are easily collected and organized through better information processing in cyberspace, helping business owners, retailers, and logistic companies. Third, cyberspace makes enormous innovation for the economy where opportunities to open businesses using the internet platform cost little to none. Digital products such as digital music (e.g. Spotify, Apple Music, Tidal), e-books, and online news and data have also boosted the growth of economy.

Access to information is a fundamental human right.[69] Cyberspace as a platform gives access to information in a more efficient, faster, and cheaper way. Cyberspace today has access to digital libraries, encyclopaedias, news, art galleries, online classes, and many other sources of information from anywhere in the world in a matter of a few clicks, promoting education, awareness, and health. Cyberspace has enabled users to take an active role in choosing what, how, and when information is gained. Information in this platform can comprise images, videos, sound, and/or text; making information easier to be spread and understood.

Many aspects of communication have outstandingly improved with the existence of cyberspace; mainly speed and time, cost, job creations, globalization, entertainment, spread of information, and business opportunities. Through cyberspace, communication becomes cheaper and faster with messages being sent and received instantly within a few clicks, which also saves the cost of communication. The improved and new form of communication creates jobs, some even new such as computer programmers, web designers, software developers, system analysts, and many more. Furthermore, the existence of

[66] Purplesec, *2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends*, Purplesec (Purplesec, 2021), https://purplesec.us/resources/cyber-security-statistics/.

[67] U M Mbanaso and E S Dandaura, *The Cyberspace: Redefining A New World*, IOSR Journal of Computer Engineering 17, no. 3 (2015), p. 18.

[68] World Bank, *World Development Report 2016: Digital Dividends* (Washington District Columbia: World Bank, 2016), p. 42, https://doi.org/10.1596/978-1-4648-0671-1.

[69] UNGA, *Universal Declaration of Human Rights*, Article 19.

social media platforms (e.g. Twitter, Facebook, Tiktok, Youtube, Instagram) not only significantly improves communication, the spread of information, and freedom of speech, but also provides entertainment for users. And as stated and explained above, cyberspace continually improves the communication, spread of information, and management within business and the education sectors.

Although opportunities from cyberspace have impacted the human lives immensely for decades, the absence of ethics in cyberspace will greatly imbalance these opportunities. This will result in negative effects having a greater impact than the positive impacts for the users within cyberspace. Without ethics, the misuse of those opportunities will cause more damage and destruction to humans. Cyberspace, made to improve human lives, would become an unsafe and treacherous place. The reflection of cyberspace, which is its unethical users, will be a great danger and threat especially with the fast advancement of technology when paired with the slower paced development of laws and regulations, as ethics are fundamental for the law at issue. There exists an urgency on ethics being implemented more in the use of cyberspace, as it has been proven on how ethics are only shown its necessity in one third of documents in relation to internet governance.

4. Between Freedom and Protection

To understand where ethics is positioned within the normative framework of cyberspace governance, two respective approaches must be analyse: the cyber freedom (cyber liberalist) and the cyber protectionist. Both perspectives will be contextualized in the example of the governance model of the United States and China. The first part of this section will deal with the cyber freedom, before proceeding to the protectionist. Only then where we will be able to seek for an ideal place to position the ethical aspects.

The history of Cyber Freedom laid in the foundation of the internet wherein 1960s, researchers from the US military established the fundamentals of the internet.[70] Since then, universities, private institutions, and private entities have joined in a haphazard, organic, and decentralized manner.[71] However, countries, including the US, have a significant role in regulating it despite its inclusive nature.[72] Within this article's context, 'cyber freedom' is understood as a multi-stakeholder governance approach for the cyberspace. Multi-stakeholder governance is popular among countries in which libertarian ideas are popular. Its factions include Free Culture, Global Public Good (GPG), Maximalist, and Anti-Marketization.[73] Aside from the US, the United Kingdom (UK), Canada, and the European Union members (EU) are known proponents of the multi-stakeholder regime.[74]

[70] Zhixiong Huang and Kubo Mačák, *Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches*, Chinese Journal of International Law 16, no. 2 (June 1, 2017), para. 29, https://doi.org/10.1093/chinesejil/jmx011.

[71] *Ibidem*.

[72] *Idem*, para. 30.

[73] Jean Marie Chenou, *From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-Stakeholderism, and the Institutionalisation of Internet Governance in the 1990s*, Globalizations 11, no. 2 (2014), p. 209, https://doi.org/10.1080/14747731.2014.887387.

[74] Huang and Mačák, *Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches*, para. 33.

The discourse on how to regulate the internet enters a libertarian popular outlook in the 1990s with the statement of David Clark, an MIT computer science professor. He expressed a government-free governance model for the internet as the overall outcome for internet regulation.[75] At that time, the internet has less than a million users.[76] The popularization of multi-stakeholder governance gains global recognition in UNGA Resolution, 57/239 of 2002. Known stakeholders include "*…governments, businesses, other organizations and individual users who develop, own, provide, manage, service and use information systems and networks…*".[77] Multi-stakeholder governance is famous for its inclusive and representative principles where stakeholders could produce norms and set standards, and define penalties and repercussions for violations.[78]

The multi-stakeholder approach is so popular that it influences current discourse in the UN about cyberspace governance. Recent developments within UN discussions are the roles of these stakeholders. These roles consist of stakeholders as influencers of opinions, problem solvers, contributors, decision-makers, sponsors of national engagement, and whistle-blowers.[79] Aside from the UN, the US also utilizes a multi-stakeholder approach in its 'Internet Freedom' diplomacy to increase the protection of human rights in cyberspace.[80] All of these is credited to the libertarian influence in the US during the 90s for influencing the internet regulatory approach. Four stakeholders are contributing to the libertarian system in regulating cyberspace: the learned society which develops and manages internet since its inception; corporates that defends an unregulated and private-sector-led market creation process; US political institutions that desire a leading role in internet policy; transnational actors intending to internationalize and take part in internet governance.[81]

It is essential to keep in mind that although cyber freedom is associated with the US by their multi-stakeholder practice, the US does not embrace it fully as they need to strike a balance that suits their interests. The US PATRIOT Act encourages ISPs (Internet Service Providers) to block website contents inconsistent with US public interest, turn over emails that reveal suspicious intent, and encourage telecommunications companies to conduct data mining on anti-terrorism grounds.[82] A real-life example is the US's blocking of three Iraq television stations in 2010 because its contents are 'anti-American'.[83]

Nevertheless, Americans are hostile to censorship, and the attitude of the US government remains receptive to unfiltered information if it does not contradict national security. All these thanks to a cornerstone value within US society: freedom of

[75] Huang and Mačák, para. 30.

[76] A Liaropoulos, *Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-Stakeholderism, and Power Politics*, Journal of Information Warfare 15, no. 4 (2016), p. 18.

[77] Liaropoulos, p. 20.

[78] *Ibidem.*

[79] Bruno Lete, *Shaping Inclusive Governance In Cyberspace*, Washington, 2019, pp. 6-10.

[80] Bureau of Democracy Human Rights and Labor, *Internet Freedom*, 2019.

[81] Chenou, *From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-Stakeholderism, and the Institutionalisation of Internet Governance in the 1990s*, p. 210.

[82] Barney Warf, *Geographies of Global Internet Censorship*, GeoJournal 76, no. 1, February 23, 2011, p. 18, https://doi.org/10.1007/s10708-010-9393-3.

[83] Binxing Fang, *Cyberspace Sovereignty*, 1st ed., Singapore, Springer Singapore, 2018, p. 97, https://doi.org/10.1007/978-981-13-0320-3.

expression. Freedom of expression is a freedom enjoyed by individuals as a medium of political orientation and culture.[84] Such values are central to US national history and collective consciousness,[85] a factor contributing to the growth of libertarian ideas in the US. For instance, citizens of the US are free to criticize their government. The US government does not take punitive action and even supports the medium of cyberspace as a place of criticism.[86] Indeed, the First Amendment of the US Constitution guarantees freedom of expression except for fraud, obscenities, defamation, and incitement.[87] US is even laxer in cyberspace, as the US government immunizes content providers (YouTube, Facebook, etc.) from the actions of their users should consider an exception to freedom of expression occurs.[88]

Yet two controversies exist from the cyber freedom concept implemented under the US. First, the US government's controversial actions in the implementation of cyber freedom policies. Second, concept of cyber freedom and the US' actions upon it. First, there is evidence that media outlets in the US, while not criminalized for expressing their views, are pressured financially and politically on their news coverage.[89] Hence, manipulating the right to free expression to the financer's interests. Another issue is the FISA Amendments Act of 2008 that permits the US government to conduct surveillance on foreigners outside the US.[90] Second, on the controversy of cyber freedom itself. While it is indeed morally 'good' to implement the cyber freedom concept to national policies, a question arises whether it is justified to pressure other countries to do so? Especially for a country with cyberspace restrictions such as the US compared to EU countries with no internet ban.[91] Another issue is the disinformation potentials and bots that manipulate public opinion in cyberspace.[92] The issue of criminalizing disinformation and bots is a challenge to proponents of cyber freedom.

Unlike cyber freedom, what we termed as the cyber protectionist concept is that countries must govern cyberspace instead of applying sovereignty in cyberspace. Cyber protectionist here is also known as cyber sovereignty proponents. The idea is popular in China, where it relies on two principles: unwanted influence in country's cyberspace must be banned and shifting internet multistakeholder governance to an international forum.[93]

The history of the cyber protectionist idea began in 2002. During the UN's World Summit on the Information Society (WSIS), there are confrontations on governing

[84] Mauricio J. Alvarez and Markus Kemmelmeier, *Free Speech as a Cultural Value in the United States*, Journal of Social and Political Psychology 5, no. 2 (2018), pp. 725-726, https://doi.org/10.5964/jspp.v5i2.590.

[85] Alvarez and Kemmelmeier, *Free Speech as a Cultural Value in the United States*.

[86] Bureau of Democracy Human Rights and Labor, *Internet Freedom*.

[87] Fernando Nunez, *Disinformation Legislation and Freedom of Expression*, UC Irvine Law Review 10, no. 2 (2019), pp. 789-790.

[88] Nunez, *Disinformation Legislation and Freedom of Expression*.

[89] Ayhan Dolunay, Fevzi Kasap, and Gökçe Keçeci, *Freedom of Mass Communication in the Digital Age in the Case of the Internet: 'Freedom House' and the USA Example*, Sustainability 9, no. 10, October 7, 2017, p. 18, https://doi.org/10.3390/su9101739.

[90] Dolunay, Kasap, and Keçeci, *Freedom of Mass Communication in the Digital Age in the Case of the Internet: 'Freedom House' and the USA Example*.

[91] Dolunay, Kasap, and Keçeci, *op. cit.*, p. 13.

[92] Nunez, *Disinformation Legislation and Freedom of Expression*, pp. 791-794.

[93] Niels Nagelhus Schia and Lars Gjesvik, *China's Cyber Sovereignty (Policy Brief)*, Olso, 2017, p. 1, https://doi.org/10.13140/RG.2.2.30512.15360.

cyberspace between multistakeholder and their opponents.[94] There are two problems: the Internet Corporation for Assigned Names and Numbers' (ICANN) ability to make Domain Name System (DNS) policies and ICANN's special authority held by the United States (US) as ICANN is the US made institution.[95]

The core philosophy in applying sovereignty to cyberspace is similar to the traditional notions of sovereignty. Proponents of cyber protectionism argue for using state jurisdiction to constituting cyberspace facilities, carrying data, and operations of data in cyberspace where state judicial and administrative institutions could exercise their power over cyberspace.[96] Hence, every sovereign state has the right and duties to not interfere with other states' cyberspace and protect its cyberspace against aggression.[97] Cyber protectionists are composed of several factions, including reformists, neoliberal proponents of cybersecurity, and sovereigntists.[98]

Proponents of the cyber protectionist concept emerge as a reaction to the cyber freedom multistakeholder approach, including countries such as China, Russia, Cuba, Iran, Saudi Arabia, Bahrain, United Arab Emirates (UAE), Iraq, and Sudan.[99] Countries, such as China, viewed the multistakeholder approach as defective in the platform with limits to authorization, function, and interest equity.[100] Furthermore, the multistakeholder approach framework is lacking in both design and coordination.[101] Hence, because of perceived defects in the cyber freedom concept, some countries prefer a protectionist attitude to cyberspace to be the way forward. China, Brazil, South Africa, and India advocates in removing ICANN's existing organization and power, then integrating it into the UN, and sharing internet jurisdiction but were unsuccessful due to multistakeholder proponents from western countries' rejection.[102] US actions on the duration of WSIS in embedding internet infrastructure to its national interest show a hegemonic condition in this supposedly free multistakeholder approach.[103] The US views for hegemony by confirming its role in internet servers' supervision.[104]

Subsequent years followed by attempts from developing countries and proponents of a multilateral approach to revoke US' control over cyberspace and several so-called 'authoritarian' states to block and filter the internet.[105] Yet, the multistakeholder approach is the championed cause by proponents' states and heavily influences the UN discourse. The overwhelming power of the multistakeholder system does not

[94] Milton L. Mueller, *Against Sovereignty in Cyberspace*, International Studies Review 22, no. 4, November 26, 2020, p. 3, https://doi.org/10.1093/isr/viz044.

[95] *Ibidem.*

[96] Fang, *Cyberspace Sovereignty*, pp. 85-86.

[97] *Idem*, p. 86.

[98] Chenou, *From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-Stakeholderism, and the Institutionalisation of Internet Governance in the 1990s*, p. 209.

[99] Roxana Radu, *Negotiating Internet Governance*, Oxford, Oxford University Press, 2019, p. 199; Huang and Mačák, *Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches*, paras. 36–37.

[100] Huang and Mačák, para. 35.

[101] *Ibidem.*

[102] Fang, *Cyberspace Sovereignty*, pp. 94-95.

[103] Fang, p. 95.

[104] *Ibidem.*

[105] Fang, pp. 95-96; Mueller, *Against Sovereignty in Cyberspace*, p. 3.

prevent multilateral proponents from working with the existing platform, such as the Internet Governance Forum (IGF).[106]

Current developments of the cyber protectionist agenda are domain name jurisdiction, data ownership rights, big data, different judging legality principles, and cyber-attacks.[107] Yet, there is indeed a concern about the nature of cyber protectionism itself. Should the role of countries become too big, this may disturb day-to-day social life due to the current interconnected nature of this globalized world. Potential problems include the defunct Autonomous Systems (AS) due to varying state regulations, removal of transnational organizations from domain administration, the emergence of national online checkpoints, the overabundance of certification demand, and strict data localization requirements.[108] It is crucial to balance state sovereignty and practicality for cyber protectionist proponents.

One could argue that China's receptiveness' to empower their cyberspace sovereignty was a product of the Confucian influence. Confucian principles are both traditional Chinese philosophical and ethical systems. Confucian principles lead to a paternalistic governance method where political leaders live by example. It attaches the government to govern with virtuous actions. As a consequence, the people could 'overturn' the government for not fulfilling their obligations according to Confucian principles.[109] Hence, government care and performance in adhering to the Confucian principles are more important than political freedom, such as fair and free elections.[110]

Chinese attitudes to censorship are mixed. The dissenters argue that censorship is a repressive measure employed by the Chinese government to maintain social control.[111] Censorship also could be used to downplay health crisis as what happened in HIV/AIDS and SARS incidents in China.[112] Furthermore, censorship makes it difficult for ordinary citizens to communicate and seek information in their everyday lives.[113] Aside from negatives, there are proponents among ordinary Chinese citizens on censorship policies even if they mostly dislike it personally.[114]

The censorship policy becomes ineffective if a citizen uses substitute words such as typos, emoticons, and wordplay, making communication somewhat more fun.[115] Moreover, censorship is not universal in all online activities, but merely concerns political events and government decisions and hence is not too intrusive.[116] There are

[106] Radu, *Negotiating Internet Governance*, p. 126; Fang, *Cyberspace Sovereignty*, p. 96.
[107] Fang, pp. 105-114.
[108] Mueller, *Against Sovereignty in Cyberspace*, pp. 14-15.
[109] Yubo Kou, Bryan Semaan, and Bonnie Nardi, *A Confucian Look at Internet Censorship in China*, in Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10513 LNCS, 2017, p. 380, https://doi.org/10.1007/978-3-319-67744-6_25.
[110] Kou, Semaan, and Nardi, p. 380.
[111] Lydia Khalil, *Digital Authoritarianism, China and COVID*, Lowy Institute Analysis (Sydney, 2020), pp. 6-7; Kadri Kaska, Hendrick Beckvard, and Tomáš Minárik, *Huawei, 5G and China as a Security Threat*, The NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2019, p. 11.
[112] Alana Maurushat, *The Benevolent Health Worm: Comparing Western Human Rights-Based Ethics and Confucian Duty-Based Moral Philosophy*, Ethics and Information Technology 10, no. 1 (2008), p. 14, https://doi.org/10.1007/s10676-008-9150-1.
[113] Kou, Semaan, and Nardi, *A Confucian Look at Internet Censorship in China*.
[114] Kou, Semaan, and Nardi, *op. cit.*, p. 385.
[115] *Idem*, p.385-386.
[116] *Idem*, p.386.

even instances where censorship proves to be beneficial for Chinese citizens.

Ordinary Chinese citizens saw benefits in government policy of censorship. On one occasion, a student posts an online hoax that the city child traffickers are rife. Before government clarification, parents came to their children's school to take their children home in droves, causing traffic jams in the process.[117] Another recurring issue is the attitudes of Chinese citizens, especially young people who act recklessly on the internet. This recklessness results in harmful internet interactions and discord among citizens, which were better left unsaid.[118] Finally, China did listen to its citizens to govern criticism as online information and opinions are the sources to improve governance and gain legitimacy—Chinese censorship is not draconian as what was voiced by dissenters.[119]

However, there is a legitimate concern over China's cyber sovereignty measures regarding cyber protectionist concept policies. These issues range from cyber espionage, intrusive authoritarian policies currently employed by China, and potential discourse on cyber sovereignty. On cyber espionage, China has a policy of media warfare which boldened after Snowden's revelations in 2013.[120] A prominent case in this is Huawei espionage allegations which the US could not prove but heavily suspect.[121] The US cannot prove espionage even as the law states that Chinese companies must cooperate with Chinese authorities for national security and intelligence reasons.[122] China also implements intrusive policies for cyberspace information system providers. It has the most extensive surveillance system globally. It monitors citizens by a geographic information system, linking cameras by IoT (smartphones, vehicles, television, etc.) to be part of the public surveillance system.[123] China's social credit system could also deter criticism against the government, nullifying censorship benefits.[124] These shortcomings could lead to an overweight of sovereignty in cyber protectionist discourse. Instead of state protection, cyberspace would be a draconian tool to control the masses.

5. The way towards equilibrium

As reiterated earlier, ethics in cyberspace expect a system of standards that enforces moral values, signifying the preservation of freedom of expression, intellectual property, and privacy. Governments must question whether the legal framework has sufficed to guarantee these standards but still at the same time respects their boundaries for sovereignty. The core values that shall be embedded in cyberspace must always refer to equality and inclusivity. There is a need for better moderation and steps to be taken in order to resolve differences in the governance model, role of state in cyberspace, developing an information culture between governments to suit the needs of filters and censorships.

The preeminent starting line will obviously be given for the right to privacy

[117] *Idem*, p. 388.
[118] *Idem*, p. 389
[119] Aimin Qi, Guosong Shao, and Wentong Zheng, *Assessing China's Cybersecurity Law*, Computer Law & Security Review 34, no. 6, December 2018, p. 1353, https://doi.org/10.1016/j.clsr.2018.08.007.
[120] Emilio Iasiello, *China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities*, Journal of Strategic Security 9, no. 2, June 2016, p. 54, https://doi.org/10.5038/1944-0472.9.2.1489.
[121] *Ibidem.*
[122] Khalil, *Digital Authoritarianism, China and COVID*, p. 9.
[123] *Idem*, p. 10.
[124] *Idem*, pp. 11-12.

and freedom are fundamental human rights. The right to privacy hinders the government and private actions from breaching the privacy of individuals where they are free from interruption or intrusion and can control the time and manner of the disclosure of their personal information.[125] Freedom in cyberspace, on the other hand, encompasses many different types of freedom, with freedom of expression as one of the core freedoms in cyberspace. Despite the utmost importance of privacy, rights and freedom of expression, limitations to both must be written and drawn clearly.

Freedom of expression is regulated under the International Covenant on Civil and Political Rights (ICCPR), stating the right to freedom of expression where this right includes freedom to seek, receive, and impart information and ideas of all kinds through any media.[126] Consequently, the article further permits limitations on such rights where the limitations must be provided by law, in order to ensure legality, and necessary for respect of the rights or reputations of others, for the protection of national security, public order, or public health or morals.[127] Furthermore, there are a range of rights that may be possible justifications for limitations on the freedom of expression,[128] such as freedom from discrimination, freedom from cruel, inhuman, or degrading treatment, the right of children to special protection, and the freedom of privacy. When freedom of expression endangers and/or violates the freedoms listed previously, the limitations on the freedom of expression shall be deemed as justified and lawful.

Right to privacy is also regulated under ICCPR where it states that no one shall be subjected to arbitrary or unlawful interference with their privacy and everyone has the right to the protection of the law against such interference.[129] Even if limitations to the rights to privacy are not explicitly stated in the ICCPR, those limitations still exist and are provided by the United Nations General Assembly (UNGA). The limitations provided have several criteria where, first, it must be provided by the law and such law must be accessible sufficiently, clear, and precise so that any individual may be certain who is authorized to conduct limitations of privacy rights when looking at the law. Second, most importantly, the limitation to privacy rights must be consistent with human rights.[130] The limitations furthermore must be necessary for reaching a legitimate aim, is proportionate to the aim, and must be the least intrusive option available.[131] If the limitations do not meet these criteria, the limitations would be deemed as unlawful and/or the interference to privacy shall be deemed as arbitrary.

Cyberspace promotes equality and inclusivity, as seen in the threshold upheld

[125] Verma and Mittal, *Legal Dimensions of Cyberspace*, p. 451.

[126] UNGA, *International Covenant on Civil and Political Rights,* Article 19 (2).

[127] UNGA, Article 19 (3).

[128] Australian Human Rights Commission, *4 Permissible Limitations of the ICCPR Right to Freedom of Expression*, Australian Human Rights Commission, Australian Human Rights Commission, 2011, https://humanrights.gov.au/our-work/4-permissible-limitations-iccpr-right-freedom-expression.

[129] UNGA, *International Covenant on Civil and Political Rights,* Article 17.

[130] Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights,* (Office of the High Commissioner for Human Rights, June 30, 2014, para. 23.

[131] UNHRC, *General Comment No. 27 - Freedom of Movement*, 1999, paras. 11–16; UNHRC, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, A/HRC/14/46*, 2010, pp. 17-18.

by United Nations,[132] as well as with the characteristics cyberspace itself which helps by providing access towards information for every of its users. The notion of equality and inclusivity in cyberspace, however, will of course result in perpetrators who violate such rights, committing cybercrimes. Cybercrimes vary from hacking, spreading hate, and misusing personal information to distributing child pornography, grooming and terrorism.[133] Penalties for cybercrimes are also similar in many countries such as large amount of fine, imprisonment depending on the severity of the cybercrime, and also the obligation to provide restitution for the victims in some countries like in the United States,[134] and reparation like in Europe.[135]

No one should be excluded from cyberspace nor be deprived from the right to access cyberspace even if one is or was a perpetrator of cybercrime. However, there are few cases where people are deprived of such right, fully and partially. The first case occurs in North Korea where its people are fully prevented from accessing the internet, having gone through extreme lengths where the government fully controls and limits the access.[136] Second, in China, the internet is available, but most used platforms—such as Google, Facebook, Instagram, Twitter—are not accessible and need virtual private network (VPN) in order to access those.[137] There have been no news of other states, other than North Korea and China, excluding its people partially nor fully from cyberspace, even as a form of punishment.

China's example of cyberspace governance shows that there are policies in pursuing a multilateralism approach that needs moderation on the extent of rights to privacy and freedom. The goal in moderating protectionist policies is urgent to prevent a possibility of an excessive role by the state that sacrifices inclusivity in governing cyberspace, which could result in cyberspace becoming a population control tool instead of a means to protect the state in this digital era. Solutions to moderation are present in the discourse between multilateral and multi-stakeholder approaches.

First, to resolve differences in governance models, each proponent must coordinate and negotiate. Coordination and negotiation between proponents are possible because the differences between multilateral protectionist methods and the multi-stakeholder libertarian approach are not about governance but rather the role of state government in the governance structure.[138] Mutual coordination and negotiation in international forums could be the bedrock to build global cyberspace governance methods using the medium of cyberspace convention and creating a sustainable

[132] International Telecommunication Union, *ICTs for a Sustainable World #ICT4SDG*.

[133] Government of the Netherlands, *Forms of Cybercrime*, Government of the Netherlands, 2021, https://www.government.nl/topics/cybercrime/forms-of-cybercrime.

[134] Adam M. Bossler, *Cybercrime Legislation in the United States*, in The Palgrave Handbook of International Cybercrime and Cyberdeviance, Cham, Springer International Publishing, 2020, pp. 257-280, https://doi.org/10.1007/978-3-319-78440-3_3.

[135] Jean-Claude Juncker, *Strengthening Victims' Rights: From Compensation To Reparation For a New EU Victims' Rights Strategy 2020-2025*, Luxembourg, 2019.

[136] Robert R. King, *North Koreans Want External Information, But Kim Jong-Un Seeks to Limit Access*, Center for Strategic & International Studies, 2019.

[137] Alice Su and Frank Shyong, *The Chinese and Non-Chinese Internet Are Two Worlds. Here's What It's like to Use Both*, Los Angeles Times, June 3, 2019.

[138] Chinese Academy of Cyberspace Studies, *International Cyberspace Governance*, in World Internet Development Report 2019, Singapore, Springer Singapore, 2021, p. 148, https://doi.org/10.1007/978-981-33-6938-2_8.

cyberspace environment by coexistence.[139] A real example of coordination and negotiation is present during UN World Summit on Information Society in 2015, where the event outcome document includes the multilateral approach as a compromise.[140]

Second, to further check the state role in cyberspace, inclusivity is paramount. Inclusivity does not mean changing to a bottom-top governance model but rather empowering cyberspace civil societies. A method to empower cyberspace civil societies is by guaranteeing formal and substantive equality for their role as a watchdog. Formal equality means treating cyberspace civil societies alike[141] by making legal stipulations to ensure their right to criticize the government. Substantive equality means ensuring results where equality is manifest.[142] A way to create results is to prevent possible criminalization when a citizen exercise their right to criticize. Two steps are essential to ensure a successful application: to develop an open culture within government to accept criticism and then to revoke or modify laws that could hinder civil societies from criticizing government actions.[143]

Developing a culture within the government to accept criticism could happen by making sure the civil societies and citizens are free from consequences over a critic, especially for a country that mandates real name online personas such as China and South Korea.[144] For affairs in modifying or revoking laws that could potentially penalize critics, examples of such laws include the Chinese Cybersecurity Law Article 48, which obliges individuals and organizations not to share information forbidden by laws or administrative regulations.[145] Yet, it is still unclear which information is permissible and not; this creates a chilling effect on critics.[146] Another example is the Indonesian Information Technology and Electronics Law 2016 *jo* 2008 (UU ITE), where its Articles 27(1), 27(3), and 28(2) have extensive interpretations that threaten legal sanction over critics.[147]

Third, it is crucial for governments to conduct measures to censor as little information as possible and are unintrusive to citizens' daily life. An example of that situation was prevalent in China, where citizens could not access information because of 'political sensitivity' locally but could access such information from their friends abroad.[148] This loophole renders censorship measures redundant and only intrude on citizens' daily life. While regarding unintrusive censorship, citizens must be free from long-term consequences of their violation of censorship rules. For

[139] Asoke Mukerji, *The Need for an International Convention on Cyberspace*, Horizons: Journal of International Relations and Sustainable Development SPRING, no. 16 (2020), pp. 198–209; Chinese Academy of Cyberspace Studies, *International Cyberspace Governance*.

[140] Huang and Mačák, *Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches*, para. 37.

[141] Jonathon Penney, *Virtual Inequality: Challenges for the Net's Lost Founding Value*, Northwestern Journal of Technology and Intellectual Property, 10, no. 3, 2012, para. 56.

[142] Penney, para. 56.

[143] Qi, Shao, and Zheng, *Assessing China's Cybersecurity Law*, p. 1353.

[144] *Ibidem.*

[145] *Ibidem.*

[146] Kou, Semaan, and Nardi, *A Confucian Look at Internet Censorship in China*, p. 381.

[147] Nur Rahmawati, Muslichatun Muslichatun, and M Marizal, *Kebebasan Berpendapat Terhadap Pemerintah Melalui Media Sosial Dalam Perspektif Uu Ite*, Widya Pranata Hukum : Jurnal Kajian Dan Penelitian Hukum 3, no. 1, 2021, p. 73, https://doi.org/10.37631/widyapranata.v3i1.270.

[148] Qi, Shao, and Zheng, *Assessing China's Cybersecurity Law*, p. 373.

example, there should not be a behavior-inducing tool that prevents citizens from critics. China Social Credit System (SCS) is an unfortunate example where a tool was designed for rendering commercial trustworthiness,[149] and is expanding to be a tool of political censorship.[150] Hence, censorship measures must be minimal, reserved for information threatening the state's livelihood, and not be behavior-inducing so as not to deter critics and unintrusive.

6. Conclusion

From a quick glance, cyberspace may merely seem a personal computer connected to the internet. However, if a broader outlook is taken, there are political, social, economic, cultural, and financial elements that have their own significant portions in the cyberspace. The borderless nature and flexibility of cyberspace requires a balance in its governance, that neither prevails absolute freedom nor authoritarian restraints. The regulability of cyberspace refers to the ability of a government to regulate the behavior of its citizens on the internet. Internet governance includes issues directly related to the technical administration of electronic resources, including private entities, as well as any and all actions performed by state authorities using legal instruments and international organizations exerting a direct impact on activities performed using the electronic medium, including those outside a regulating state

This article has analyzed the inherent relationship that exists between cyber ethics and its governance. It is impossible to emit moral values from any normative framework if one government seeks to control it. Order can only emerge from incepting the appropriate human values that will act as a tool for virtual control between netizens in cyberspace. In this sense, the ideal model would balance between giving the liberty for users to access and utilizing cyberspace to the greatest of their benefits. Concurrently, it is necessary to also limit such liberty so that it would not create chaos. This refers to four integral issues that become a problem between freeing and protecting internet users in the areas of: free speech, IPR, privacy, and security.

Fortunately, there are two noticeable approaches that has been taken by countries such as the US and China, where the prior emphasizes on freedom, and the later stresses its protection. We have discovered that even the most liberalizing governance still encounter problems with their multi-stake holder approach, particularly with the issues of disinformation and free speech. On the contrary, protectionist countries are faced with cyber espionage, intrusive authoritarian policies that endanger the citizen's right to access information and privacy. We propose that two concepts must be harmonized, in that an urgency for moderating the freedom and protection would be put on balance. Our solutions have taken a general approach which covers the needs for states to resolve their differences in their governance model by conducting further coordination and negotiation between government and stakeholders, re-affirming the role of governments in exercising sovereignty, and developing a culture of equality and inclusivity within the cyberspace.

[149] Fan Liang et al., *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, Policy & Internet 10, no. 4, December 2018, p. 416, https://doi.org/10.1002/poi3.183.

[150] *Idem*, pp. 435-436.

References

- Aaronson, Susan Ariel, *What Are We Talking about When We Talk about Digital Protectionism?*, World Trade Review 18, no. 4, August 6, 2019, https://doi.org/10.1017/S1474745618000198;
- Alvarez, Mauricio J., and Markus Kemmelmeier, *Free Speech as a Cultural Value in the United States*, Journal of Social and Political Psychology 5, no. 2, 2018, https://doi.org/10.5964/jspp.v5i2.590;
- ASEAN Secretariat, *ASEAN Human Rights Declaration and Phnom Penh Statement on the Adoption of the ASEAN Human Rights Declaration*, Phnom Penh, Association of Southeast Asian Nations, 2012;
- Asyari, Haekal Al., *Cyberspace as a Common Heritage of Makind: Governing Jurisdictional Limitations of the Internet by Virtue of International Law*, University of Debrecen, 2020;
- Australian Human Rights Commission, *4 Permissible Limitations of the ICCPR Right to Freedom of Expression*, Australian Human Rights Commission. Australian Human Rights Commission, 2011, https://humanrights.gov.au/our-work/4-permissible-limitations-iccpr-right-freedom-expression;
- Bailey, Diane, *Cyber Ethics*, `1 New York, The Rosen Publishing Group, 2008;
- Bauman, Zygmunt, *Morality without Ethics*, Theory, Culture & Society 11, no. 4, November 29, 1994, https://doi.org/10.1177/026327694011004001;
- Bordo, Michel D., Alan M.Taylor, and Jeffrey G. Williamson, eds., *Globalization in Historical Perspective*, Chicago, University of Chicago Press, 2003;
- Bossler, Adam M., *Cybercrime Legislation in the United States*, in The Palgrave Handbook of International Cybercrime and Cyberdeviance, Cham, Springer International Publishing, 2020, https://doi.org/10.1007/978-3-319-78440-3_3;
- Bureau of Democracy Human Rights and Labor, *Internet Freedom*, 2019;
- Buttigieg, Jean, *The Common Heritage of Mankind From the Law of the Sea to the Human Genome and Cyberspace*, Symposia Melitensia 8, Special Issue, 2012;
- Chenou, Jean Marie, *From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-Stakeholderism, and the Institutionalisation of Internet Governance in the 1990s.*, Globalizations 11, no. 2/2014, https://doi.org/10.1080/14747731.2014.887387;
- Chinese Academy of Cyberspace Studies, *International Cyberspace Governance*, in World Internet Development Report 2019, Singapore, Springer Singapore, 2021, https://doi.org/10.1007/978-981-33-6938-2_8;
- Christoph, Stuckelberger, and Duggal Pavan, *Cyber Ethics 4.0: Serving Humanity with Values*, edited by Ignace Haaz and Samuel Davies, Geneva, Globethics.net, 2018;
- Clarke, Roger, *Ethics and the Internet: The Cyberspace Behaviour of People, Communities and Organisations*, Business and Professional Ethics Journal 18, no. 3 & 4/1999, https://doi.org/10.5840/bpej1999183/423;
- CNN Indonesia, *Sebut Netizen RI Paling Tidak Sopan Akun Microsoft Diserang*, CNN Indonesia. Jakarta, 2021, https://www.cnnindonesia.com/teknologi/20210226140821-192-611309/sebut-netizen-ri-paling-tidak-sopan-akun-microsoft-diserang;
- Council of Europe, *Budapest Convention on Cybercrime*, European Treaty Series - No. 185, 2001;
- Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, European Treaty Series - No. 108, 1981;
- Directive 2016/680 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of

criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Official Journal of the European Union, 2016;

- European Convention on Human Rights, 1950;
- Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse, *Defining Cybersecurity*, Technology Innovation Management Review 4, no. 10, October 30, 2014, https://doi.org/10.22215/timreview/835;
- Dolunay, Ayhan, Fevzi Kasap, and Gökçe Keçeci, *Freedom of Mass Communication in the Digital Age in the Case of the Internet: 'Freedom House' and the USA Example*, Sustainability 9, no. 10, October 7, 2017, https://doi.org/10.3390/su9101739;
- Doneda, Danilo, and Virgilio A.F. Almeida, *Privacy Governance in Cyberspace*, IEEE Internet Computing 19, no. 3, May 2015, https://doi.org/10.1109/MIC.2015.66;
- Dudley, Alfreda, James Braman, Giovanni Vincenti, Eugenia Alexandropoulou-Egyptiadou, Anteneh Ayanso, Jonathan Bishop, Sam De Silva, et al., *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices*, edited by Lindsay Johnston Kristin Klinger Erika Carter, Myla Harty, and Sean Woznicki, 1st ed. Hershey, IGI Global, 2012;
- Fang, Binxing, *Cyberspace Sovereignty*, 1st ed., Singapore, Springer Singapore, 2018, https://doi.org/10.1007/978-981-13-0320-3;
- Fardiyan, Ahmad Rudy, *Etika Siber Dan Signifikansi Moral Dunia Maya*, in Prosiding Seminar Nasional Komunikasi: Akselerasi Pembangunan Masyarakat Lokal Melalui Komunikasi Dan Teknologi Informasi, Lampung, Universitas Lampung, 2016;
- Fletcher, George P., *Law and Morality: A Kantian Perspective*, Columbia Law Review 87, no. 3, April 1987, https://doi.org/10.2307/1122670;
- Goi, Chai Lee, *Cyberculture: Impacts on Netizen*, Asian Culture and History 1, no. 2, July 1, 2009, https://doi.org/10.5539/ach.v1n2p140;
- Government of the Netherlands, *Forms of Cybercrime*, Government of the Netherlands, 2021, https://www.government.nl/topics/cybercrime/forms-of-cybercrime;
- Huang, Zhixiong, and Kubo Mačák, *Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches*, Chinese Journal of International Law 16, no. 2, June 1, 2017, https://doi.org/10.1093/chinesejil/jmx011;
- Iasiello, Emilio, *China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities*, Journal of Strategic Security 9, no. 2, June 2016, https://doi.org/10.5038/1944-0472.9.2.1489;
- Imaduddin, M. Hafidz, *Akun Instagram 'Baru' All England Langsung Diserbu Netizen Indonesia*, Kompas, 2021, https://www.kompas.com/badminton/read/2021/03/20/15491538/akun-instagram-baru-all-england-langsung-diserbu-netizen-indonesia?page=all;
- International Telecommunication Union, *ICTs for a Sustainable World #ICT4SDG*, International Telecommunication Union, 2021, https://www.itu.int/en/sustainable-world/Pages/default.aspx;
- *World Summit on the Information Society Outcome Documents, Geneva 2003 - Tunis 2005*, Geneva, Tunis, 2005;
- Juncker, Jean-Claude, *Strengthening Victims' Rights: From Compensation To Reparation For a New EU Victims' Rights Strategy 2020-2025*, Luxembourg, 2019;
- Kabay, M. E., *Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy*, in Annual Conference of the European Institute for Computer Anti-Virus Research (EICAR), Munich, 1998;
- Kaska, Kadri, Hendrick Beckvard, and Tomáš Minárik, *Huawei, 5G and China as a Security Threat*, The NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2019;
- Kaspersky, *What Is a Cookie? How It Works and Ways to Stay Safe*, 2021, https://www.kaspersky.com/resource-center/definitions/cookies;
- Khalil, Lydia, *Digital Authoritarianism, China and COVID*, Lowy Institute Analysis, Sydney, 2020;

- King, Robert R., *North Koreans Want External Information, But Kim Jong-Un Seeks to Limit Access*, Center for Strategic & International Studies, 2019;
- Kou, Yubo, Bryan Semaan, and Bonnie Nardi, *A Confucian Look at Internet Censorship in China*, in Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10513 LNCS, 2017, https://doi.org/10.1007/978-3-319-67744-6_25;
- Lamerichs, Nicolle, Dennis Nguyen, Mari Carmen, Puerta Melguizo, Radmila Radojevic, and Anna Lange-Böhmer, *Elite Male Bodies: The Circulation of Alt-Right Memes and the Framing of Politicians on Social Media*, Journal of Audiences& Reception Studies 15, no. 1, 2018;
- League of Arab States, *Arab Charter on Human Rights*, 2004;
- Lete, Bruno, *Shaping Inclusive Governance In Cyberspace*, Washington, 2019;
- Lewis, James A., *Cybersecurity and Critical Infrastructure Protection*, Center for Strategic & International Studies, 2006;
- Liang, Fan, Vishnupriya Das, Nadiya Kostyuk, and Muzammil M. Hussain, *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, Policy & Internet 10, no. 4, December 2018, https://doi.org/10.1002/poi3.183;
- Liaropoulos, A., *Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-Stakeholderism, and Power Politics*, Journal of Information Warfare 15, no. 4, 2016;
- Maurushat, Alana, *The Benevolent Health Worm: Comparing Western Human Rights-Based Ethics and Confucian Duty-Based Moral Philosophy*, Ethics and Information Technology 10, no. 1, 2008, https://doi.org/10.1007/s10676-008-9150-1;
- Mbanaso, U M, and E S Dandaura, *The Cyberspace: Redefining A New World*, IOSR Journal of Computer Engineering 17, no. 3, 2015;
- Moka-Mubelo, Willy, *Law and Morality*, in Reconciling Law and Morality in Human Rights Discourse: Beyond the Habermasian Account of Human Rights, 3, Cham Springer International Publishing, 2017;
- Mueller, Milton L., *Against Sovereignty in Cyberspace*, International Studies Review 22, no. 4, November 26, 2020, https://doi.org/10.1093/isr/viz044;
- Mukerji, Asoke, *The Need for an International Convention on Cyberspace*, Horizons, Journal of International Relations and Sustainable Development SPRING, no. 16, 2020;
- Nunez, Fernando, *Disinformation Legislation and Freedom of Expression*, UC Irvine Law Review 10, no. 2, 2019;
- Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, Office of the High Commissioner for Human Rights, June 30, 2014;
- Omotoyinbo, Femi Richard, *Online Radicalisation: The Net or the Netizen?*, Social Technologies 4, no. 1, 2014, https://doi.org/10.13165/ST-14-4-1-04;
- Organization of American States, *American Convention on Human Rights*, 1969;
- Penney, Jonathon, *Virtual Inequality: Challenges for the Net's Lost Founding Value*, Northwestern Journal of Technology and Intellectual Property 10, no. 3, 2012;
- Purplesec, *2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends*, Purplesec. 2021, https://purplesec.us/resources/cyber-security-statistics/;
- Qi, Aimin, Guosong Shao, and Wentong Zheng, *Assessing China's Cybersecurity Law*, Computer Law & Security Review 34, no. 6, December 2018, https://doi.org/10.1016/j.clsr.2018.08.007;
- Radu, Roxana, *Negotiating Internet Governance*, Oxford, Oxford University Press, 2019;
- Rahmawati, Nur, Muslichatun Muslichatun, and M Marizal, *Kebebasan Berpendapat Terhadap Pemerintah Melalui Media Sosial Dalam Perspektif Uu Ite*, Widya Pranata Hukum, Jurnal Kajian Dan Penelitian Hukum 3, no. 1/2021, https://doi.org/10.37631/widyapranata.v3i1.270;
- Rewak, William J, and Shannon Vallor, *An Introduction to Cybersecurity Ethics*, Santa Clara, Santa Clara University, 2018;

- Rizal, Muhamad, and Yanyan Yani, *Cybersecurity Policy and Its Implementation in Indonesia*, in JAS (Journal of ASEAN Studies) 4, no. 1, August 2016, https://doi.org/10.21512/jas.v4i1.967;
- Schia, Niels Nagelhus, and Lars Gjesvik, *China 's Cyber Sovereignty (Policy Brief)*, Oslo, 2017, https://doi.org/10.13140/RG.2.2.30512.15360;
- Seese, Michael, *Scrappy Information Security*, edited by Kimberly Wiefling, Silicon Valley, Happy About, 2009;
- Singh, Jerome Amir, *Sustainable Development Goals: The Role of Ethics*, Sight Life 29, 2015;
- Spinello, Richard A., *Code and Moral Values in Cyberspace*, Ethics and Information Technology 3, no. 2, 2001, https://doi.org/10.1023/A:1011854211207;
- Spinello, Richard A., *Ethics in Cyberspace: Freedom, Rights, and Cybersecurity*, in Next-Generation Ethics, Cambridge University Press, 2019, https://doi.org/10.1017/9781108616188.029;
- Su, Alice, and Frank Shyong, *The Chinese and Non-Chinese Internet Are Two Worlds. Here's What It's like to Use Both*, Los Angeles Times, June 3, 2019;
- Teresa, Fuentes-Camacho, *Introduction: UNESCO and the Law of Cyberspace*, in The International Dimensions of Cyberspace Law, 2nd ed., Routledge, 2000;
- Trachtman, Joel, *Cyberspace, Sovereignty, Jurisdiction, and Modernism*, Indiana Journal of Global Legal Studies 5, no. 2, 1998;
- Umejiaku, Nneka Obiamaka, and Mercy Ifeyinwa Anyaegbu, *Legal Framework for the Enforcement of Cyber Law and Cyber Ethics in Nigeria*, International Journal of Computers & Technology 15, no. 10 (2016), https://doi.org/10.24297/ijct.v15i10.12;
- UNGA, *International Covenant on Civil and Political Rights*, 1966;
- United Nations General Assembly Resolution *Combating the criminal misuse of information technologies*, A/RES/55/63 (2001);
- United Nations General Assembly Resolution *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*, A/RES/58/199 (2004);
- United Nations General Assembly Resolution *Creation of a Global Culture of Cyber Security*, A/RES/57/239 (2003);
- United Nations General Assembly Resolution *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*, A/RES/64/211, 2010, https://doi.org/10.1680/jdare.16.00049;
- United Nations General Assembly Resolution *The Right to Privacy in the Digital Age*, UN Doc A/RES/68/167, 2014;
- United Nations, *Universal Declaration of Human Rights*, 1949;
- UNHRC, *General Comment No. 27 - Freedom of Movement*, 1999;
- *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, A/HRC/14/46, 2010;
- United Nations Human Rights Council Decision, Panel on the Right to Privacy in the Digital Age, A/HRC/DEC/25/117, 2014;
- United Nations Human Rights Council Decision, The Right to Privacy in the Digital Age, A/HRC/28/L.27, 2015;
- United States International Trade Commission, *Digital Trade in the US and Global Economies*, Part 1, 2013;
- Verma, S K, and Raman Mittal, *Legal Dimensions of Cyberspace*, edited by S K Verma and Raman Mittal, New Delhi, Indian Law Institute, 2004;
- Warf, Barney, *Geographies of Global Internet Censorship*, GeoJournal 76, no. 1, February 23, 2011, https://doi.org/10.1007/s10708-010-9393-3;
- Weber, Rolf H., *Ethics as Pillar of Internet Governance*, Jahrbuch Für Recht Und Ethik / Annual Review of Law and Ethics 23, 2015;

- Weber, Rolf H., *Principles for Governing the Internet: A Comparative Analysis*, Paris, UNESCO Publishing, 2015;
- World Bank, *World Development Report 2016: Digital Dividends*, Washington District Columbia, World Bank, 2016, https://doi.org/10.1596/978-1-4648-0671-1;
- Zimbardo, Philip G., *The Human Choice: Individuation, Reason, and Order versus Deindividuation, Impulse, and Chaos*, in Nebraska Symposium on Motivation, University of Nebraska Press, 1969.