CYBERSPACE: THE CHALLENGE OF IMPLEMENTING A GLOBAL LEGAL FRAMEWORK THE IMPACTS OF TIME & SPACE FACTORS

Mohamad Albakjaji, Prince Sultan University

ABSTRACT

This article focuses on one of the contemporary challenging issues–it is the challenge of governing the activities that are conducted via cyberspace. In most cases governments are unable to regulate these activities that are of cross border dimensions. Although many laws have been adopted to regulate these activities, these solutions remain inadequate because they are considered national or regional initiatives rather than global ones. The aim of the current paper is to draw attention to the impact of international dimensions of cyberspace on the national and international legal systems, and to highlight the factors affecting these systems. The mechanism of time and space will be discussed in a way that explains the ability of cyberspace to cross the states' territory without taking into consideration the national and international law. Moreover, the current research will raise the issue of the absence of an international consensus on the need for adopting unified rules to govern and regulate the global cyberspace activities such as the e-commerce ones. Based on real Cyberspace case studies on international level, this paper aims to identify the main factors and reasons that hinder adopting an international framework.

Keywords: Cyberspace, Time, Space, E-Commerce, Governance and Law.

INTRODUCTION

With the invention of the internet and making it accessible to the public in 1990, a new type of communication has emerged. This led to create what we call today as a public cyberspace that relies on the Internet, which is a global and decentralized computer network system. Due to its nature, Cyberspace is considered as an international and virtual space where different users may be affected. Hence different legal systems may be involved in a case of dispute. So, applying single legal system on cyberspace will be ineffective in regulating this global space. Yet, the international law is unable to govern these activities.

However, some issues are still unsolved, examples of these are; what makes cyberspace lawless zone and why has the current national and international laws have become outdated and invalid for cyber activities? How effective are current laws in dealing with cyberthreats and activities?

This study will shed light on discussions on these fundamental research questions. Hence, it is intended to draw the attention of the international committee to the main factors that affect the effectiveness of the traditional legal system in governing and regulating the activities associated with the cyberspace internationally.

Following from the above introduction, the next section will discuss the prior research that dealt with this issue. Then section two will cover the legal and philosophical perspectives of cyberspace. Section three will spotlight on the mechanisms of time and space as they are the

main factors of cyberspace affecting the current legal system. Hence, case studies from different jurisdictions have been selected for assessing the level of effectiveness of the current national and international laws in governing the cyberspace.

LITERATURE REVIEW

Cyberspace Regulation: Prior Research

While the Cyberspace literature has often focused on researching many models of studies (security, politic, technique and legal), this paper provides a new sight on cyberspace through shedding the light on the elements of time and space and their effects on cyberspace regulation.

In terms of improving the business model and commercial activities, Lewis's research (2010) discusses the political wish of the police makers in the USA in limiting the role of the states and the international committee in cyberspace governance by focusing on encouraging companies to improve their business modules.

From the legal perspective, scholars such as Hedley (2003), Duarte (2017) and Schneider (2017) mentioned the challenges of applying a specific state law on the international dispute resulting from e-commerce activities where different laws, regulations, and policies may apply in cases of legal disputes.

In response to such challenge, some scholars call for adopting new roles such as soft roles to govern cyberspace activities (Kucklich, 2009; Choucri & Clark, 2013). This is because the traditional international rules are of a fixed nature that cannot cope with the technological development whereas soft rules are characterized by its flexibility and simple procedures.

In general, previous literature on cyberspace failed to draw attention to the impact of international characteristics of cyberspace on legal system. So, the research gap found in the literature would drive the current research into concentrating on linking the issue of effectiveness of the current international law in regulating the cyberspace activity to the issue of the dynamicity of time and space as they are the main factors of cyberspace that undermine the role of states' control over the cyberspace activities. Also, the difficulties in arriving at an international consensus on the need for laws that govern cyberspace activities will be addressed too.

Cyberspace & Real Space: Different Theoretical Perspective

Recently, the nature of cyberspace has been discussed from different points of view; ranging from a complete rejection–being considered as status of libertarian fantasy where cyberspace is not considered as real thing- to being considered as a true international space.

Firstly, Deibert et al. (2012) conceived the cyberspace as a geographically separate area. Hence, cyberspace is considered as a real, international, independent space that combines all online users in its galaxy (Sheldon, 2014).

Moreover, other researchers discussed the cyber power issue from a geographical point of view. (Sheldon, 2014) argued that the cyberspace has a geographical setting and meaning, and he stated that:

> *"The physical segment of cyberspace-the computers, cables, and satellites, among other physical infrastructure-is geographically situated and operated and maintained by human beings who must, by*

necessity, live on the land in politically organized communities in physically distinct and demarcated territories".

Finally, although there are different perspectives towards the cyberspace concept, the current legal system is not effective in governing and regulating the activities conducted online.

Time & Space Power: Continuous Violations to the Territory of the State

Due to the ubiquity of cyberspace network, information could be easily circulated throughout the world instantly. This is called the time acceleration of cyberspace. This acceleration or timelessness of cyberspace activities makes international and national laws unable to keep up to date with technological developments (Choucri & Clark, 2013). The time acceleration creates a type of legal uncertainty in the legal framework because the international law is not ready yet to govern this issue. So, using cyberspace for different purposes such as commercial, social, or even though criminal ones leads all the traditional legal systems into an abyss.

The timelessness and boundarylessness of cyberspace make it easy for the information to cross states borders without the need for visa or permission. This has an effect on the state powers of deterrence because the power of time and space of the cyberspace will undermine the ability of states to control its territory. Based on this, imposing national legislation is not enough to say that the state has an absolute sovereignty, but rather the state should have the power to impose its legislations internationally. However, this seems almost impossible because the power of the state in this area is limited.

International Law: The Issue of Uncertainty

Cyberspace has become a harbour for cybercriminal who use black webs from nowhere to start their cyber-malicious activities against states and individuals. Hence, the cybercrime can be committed from the other side of the world as easily as from next door. So, the boundarylessness of cyberspace makes the online activities as lawless zone because the current international rules and principles are not able to govern such conducts (Schmitt, 2013). According to international law codified in the U.N. Charter's Article 2(4), states are prohibited from directly or indirectly using cyber force against other states where states in their international relations among each other should respect the non-intervention principle and avoid interfering in the affairs of foreign nations. Based on this, each state has its own sovereignty and control over its territory and cyberinfrastructure to ensure that these infrastructures are not used for conducting unlawful actions against other states.

Moreover, in response to cyberoperations generated by another state, some international court jurisdictions (ICI) gave the victim state the right to respond to this operation if the victim state faces cyberoperations that pose risks and imminent peril to its essential interests. The protective measures in this case may be taken by the state, should only rely on the plea of necessity.

In this way, we can find that the ICJ and the articles of international law associated with cyberspace activities are ambiguous and may be interpreted in different ways according to the contexts and circumstances of states.

Firstly, some researchers criticised the international court because it limits the right of the state to take measures that include anticipatory or preventative self-defence against an imminent attack with respect to cyberspace to the plea of necessity. Schmitt (2013) stated that:

> *"So long as an attacker possesses the capability to conduct cyberoperations at the armed-attack level, intends to do so, and defensive operations are required immediately lest the target state lose its opportunity to defend itself, the target may resort to force in self-defence to preempt the prospective attack".*

Secondly, the ICJ does not take into consideration the cyberoperations that are conducted by non-state actors such as gangs that work online. According to ICJ, victim state can only enjoy this right if these operations are launched by other states.

Other ambiguous terms included in the international rule is that the article 51 of U.N. Charter provided that the state has the right to use force to defend its territories against the armed attacks that include cyberoperations causing death, injury, or significant damage (Hongju, 2012).

The concept of attack has been defined by the 1977 Additional Protocol I as *"acts of violence"* (Schmitt, 2013). This attack should cause injury or physical damage otherwise the victim state will lose it eight to respond. So, this interpretation is criticised because it does not cover the cyberattacks that cause damage to civilian object, or to economic interest of the state. Hence, economic loss with no physical harm is not yet taken into consideration by the international community.

Concerning the attacks that are launched by third party, the international law is not clear as well, and adopts a narrow approach. According to the art 8 of the Draft Articles, the state is not liable for these acts unless these actors act under the sate instructions, control and direction. Hongju (2012) argued that:

> *"These rules are designed to ensure that states cannot hide behind putatively private actors to engage in conduct that is internationally wrongful".*

Moreover, in a case of attack, the victim state must prove that there is a direct link between the proxies' actors and the State machinery, or these actors work under the control of the State Machinery. To proof this is not an easy task, because the ICJ adopted a narrow way in interpreting this concept. For instance, the ICJ's decision in the case of Nicaragua v United States of America limited the USA responsibility. Although Nicaragua could prove that the rebel group that launched cyberoperations against it was funded and equipped by the USA, the ICJ has limited the responsibility of the USA. So, training, and arming rebel groups by the State Machinery is the only way to prove the relationship between rebel groups and the State Machinery. Therefore, the state's responsibility for a use of force will be raised according to the article 2(4) of the UN Charter. In this regard, The Margulies (2012: 11-12) stated that:

> *"The ICJ couched these terms in its formulation of what it called an 'effective control' test. While to American ears 'effective control' may connote practical control, the ICJ's use of the term requires something closer to specific, comprehensive control."*

Moreover, he criticised the approach that has been adopted by the Draft Article, because it does not consider the funding and training actions as conducts that may raise the supporting state's responsibility. He argued that a mere financial support of the rebel group that launched a

cyber-attack against the victim state does not rise to the level of use of force (*Ibid*). In the same sense, the International Criminal Tribunal for the Former Yugoslavia (ICTY) has adopted the narrow approach that is adopted by the Draft Article. It has been decided that raising the state's responsibility requires proving the official participation of *the* supporting state where the military operations must be planned and made under the supervision of this state.

Cyberspace: A Conceptual Conflict

The main challenges that face the international community towards cyberspace issue is that the international law does not take into consideration the cross-borders nature of the cyberspace as a virtual network. Rather it only recognises states as the main entities that have the right to regulate this space. The current point of departure of the international regulations of cyberspace is the sovereignty of the state that is relied on the ability of the state to control its territory and impose laws and legislations on population who live in its territory. This weakens the ability of the international laws in governing the cyberspace activities, and ignores the role of civil, private, and social actor in governing the cyberspace conducts (Couture & Toupin, 2019). According to Bellanger (2011), state is a physical space that is limited to tangible borders, but the cyberspace is a link that is a universal one that links different single states. So, regulating the internet cannot be done unless the current international view towards the borders and sovereignty concepts is replaced by a new way of internet governance. Also, the different views of the states towards cyberspace hinder the efforts aiming at reaching an international consensus on the need for laws that govern cyberspace activities. Whereas some countries consider imposing restrictions on cyberspace activities in the name of national security interests as *a* justified and legitimate act, other states consider cyberspace as a space that may enhance the democratic values. An example of this conflict is the case of France v Yahoo (2002) where Yahoo.com (in USA) opened an online auction and displayed some items online that are related to anti-Semitic or pro-Nazi issues. This auction was displayed in all yahoo online branches including Yahoo. Fr (French webpage). French court ordered Yahoo.com to remove these items from Yahoo.fr because conducting such activities breached the French law on users' privacy that affect a large segment of society rejecting these activities. To enforce the French judgment Yahoo.com removed these items only from Yahoo.fr. However, removing these items from Yahoo.fr means that these items were still displayed on Yahoo.com because the French court and law does not have any jurisdiction in USA's territory as Yahoo.com is located and registered there. As long as these items are still displayed on Yahoo.com, therefore they are still accessible to/from everywhere around the word including France. So, removing such items from the branch company webpage did not resolve this issue. Later, the French court ordered Yahoo Company to remove it from its main website Yahoo.com. Yahoo Company filed a suit in California court to appellate the French judgement. The USA court reversed the French court on the ground that France does not have a jurisdiction on the USA's territory. So, as Yahoo.com is located and registered in USA, the USA's legal system should be applied on Yahoo.com that has the right by law to display such items because cyberspace is considered as a tool for facilitating the freedom of speech that is dedicated in the USA constitution. So, the French law was not able to resolve such cases that have international dimensions that easily can help Yahoo company to avoid the strict rules and regulations.

This case is considered as a proof that large internet engine such as Yahoo, and Google conduct commercial activities with other companies by trading our data. Usually, users are not aware of these activities because they do not have direct relationships with advertising companies. The direct relationship is well built between the internet engines, or smart devices platforms and their advertising partners. In the case against **Google (2014**), the federal trade commission (FTC) argued that Google placed cookies on the devices of Safari users who visited sites within Google's DoubleClick advertising network. So, Google collected information on the users' browsing history, sell it and then send it to its advertising partners by circumventing the protection system installed by safari (Salinas, 2018). As a penalty, Google paid a record fine of $22.5 million in a settlement with the Federal Trade Commission. Although Google paid this fine, yet Google's earnings outweighed the loss (Ziegeldorf et al., 2014). In the absence of a severe penalty, we can say that the USA's legal system governing the e-commerce activities is very lenient. This proves that the political will in the USA should improve the business module rather than impose restrictions on these large companies.

In the same way, three Safari users in the UK launched legal proceedings and invited users who had used this application on their PC, Mac, iPhone, iPad and iPod devices during the period in question. According to Broersma (2013) more than 10 million users in the UK has been affected by this breach. So, it is expected to impose on Google fine that may reach £100m. In October 2018 London's High Court ruled that Google's action was wrong, and Google breached its duty owed to the claimant. Although the court held that Google's actions were "*wrongful*", the High Court judge Mark Warby said in his ruling that Lloyd (from the Law firm that represents the claimant) had not supported his argument; that he and those represented by the campaign suffered "*damage*" as defined under data protection rules (Broersma, 2018). Also, the judge said it was difficult to calculate exactly how many people had been affected and claims they had suffered damage were not supported by the group bringing the case (BBC News, 2019).

In 2019 Claimants made an appeal, and the court of appeal in the London Now, however, the Court of Appeal has said

> *"The case can proceed, ruling that: individual personal data has a value the definition of damage could apply to loss of control of personal data, which, therefore, could qualify users for compensation representative actions of this type are a suitable legal procedure for seeking mass redress" (BBC News, 2019).*

Mr Lloyd said,

> *"The Court of Appeal has confirmed our view that representative actions are essential for holding corporate giants to account".*

Google wants now to play the same game that has already been played in previous cases. Google alleged that this case should be heard by the USA. By doing so, Google tries to move the case to its home territory where the rules governing such activities are very lenient. If Google could move the case, this means that Google will earn lots of money because the amount that Google will pay to redress the users' injury will be lesser than the ones that should be paid in the UK. Or the case could be dismissed as happened in Yahoo v France case.

In this sense, we can say that many reasons have motivated online companies to choose the USA territory to be as their headquarters, therefore, the place for resolving their disputes. In the USA, the laws governing the privacy issue are specific and sectorial ones and cover specific

fields such as the family education rights and personal medical information (Kauffma et al., 2011). Hence, it is evident that USA legal system aims to protect users from the governmental intrusion where the freedom of individual from the control of the government is protected. However, in terms of personal information protection, USA approach aims to give companies the freedom of adopting a privacy policy that matches their goals and aims. So, the self-regulation approach is dominant there, where the role of the government is limited in the event of egregious breaches of privacy. This make the USA rules more reactive rather than being preventative (Pardau & Edwards, 2017) whereas in the UK, the rules governing the privacy right are stricter ones than the American approach (Albakjaji et al., 2020).

The focus of the EU legal system is the protection of individuals from the misuse of personal information which are collected by businesses, while the USA legal system aims to protect the individual privacy against the intrusion made by the government rather than that made by the private sector. Thus, the EU system considers the privacy right as a fundamental human right, while the USA constitution does not consider this right as an explicit fundamental right (Cain, 2002; Kauffma et al., 2011). Hence, it is evident that the EU legal system aims to protect the dignity and the public image of citizens, whereas, the USA system is more interested in curbing the governmental intrusion-an aim that is driven from the libertarian thought or the freedom of individual from the governmental control. In terms of policies and practices associated with the information privacy protection, the US companies embark on applying the self-regulation approach where the company has the freedom of adopting a privacy policy that are suitable to its goals and aims, and the role of the government is limited in the event of egregious breaches of privacy. In contrast, EU companies are obliged to obtain a prior consent from the costumer before collecting or using personal information (De-Smedt et al., 2018).

The most important case that created an international conflict is the case of Google against the Chines government. In 2006 Google.cn has been launched in China but it was forced by the communist government in China to accept self-censorship (Hartnett, 2011). The motivation of this censorship is the national security interests. In accepting such censorship, Google must remove from this website any information on democracy and human rights (Brenkert, 2009). Although Google accepted working under this censorship, in 2009, Google was the victim of cyber-attack which was promoted by the Chinese government to hack the email accounts of some human rights activists. This has resulted into an international conflict between China and Google that is supported by USA. As a result of this conflict, Google in 2010 cancelled all its activities in China and redirected its activities to Hong Kong (Tan & Tan, 2012).

As mentioned earlier, we can say that each state has its own approach and view to cyberspace activities. The USA's approach that is derived from market theory rooted in John Milton's Areopagitica and John Stuart Mill's on Liberty tends to make the cyberspace as an open space to support the free trade and speech. By contrast, as a socialist nation, the Chinese approach is rooted in Marxism-Leninism with a mixture of Hegel and 19th century by which the Chinese government has a belief that cyberspace is considered as a facilitating space for free flow of information which imposes a significant threat and risk to the national security and its socialist regime.

Finally, we can say that the current international approach that is based on Westphalian system focuses on applying Cyber Westphalian system to cyberspace activities. Therefore, creating and erecting online boarders is the best way to govern and regulate the cyberspace

activities, and protect the state's national security. For this purpose, Demchak and Dombrowski (2014) stated that:

> *"Even though these alternative approaches to defining the nation's cyber borders are likely to be implemented by the national telecommunication firms and regulatory agencies, each will operate differently to establish what is and is not part of the state in cyberspace (32)."*

Although, the proponents of this approach see that creating online borders may help states in controlling cyber activities, they ignore the idea that the era of globalisation makes the world an open village. Kulesza and Balleste (2014) argued that a new approach should be applied internationally to provide a good governance of cyberspace. This new approach should be built on the shared sovereignty approach that may replace the traditional one that focuses on enhancing the single sovereign state which is the crucial architecture of the Westphalian regime. In their argument, they relied on the idea that building online fences ignores the globalisation era that makes the world open, and the states' borders are destroyed by the power of cyberspace. According to them, filtering information, creating censorship or building online gates as states borders will affect the human rights because this approach does not take into consideration that cyberspace is the main supporter of the fundamental human rights such as educational, political and civil ones as it provides the free flow of information. By dealing with the information as postal package, information will be exchanged narrowly.

CONCLUSION

From these examples and cases, it is worth mentioning the fact that the cyberspace can easily cross the borders without taking into consideration the state's regulations and laws. Usually Government regulation of the Internet is pervasive; nearly each state imposes its laws on the national level, ostensibly to protect the safety of the Internet environment and its national security (Tan & Tan, 2012); however the boundarylessness and time acceleration reduce the effectiveness of these laws nationally and internationally. Usually, the rules of international private laws that allow courts to identify which law is applicable on the dispute are unable to be applicable on cyberspace disputes due to its cross-border dimensions. This makes it impossible to apply these rules internationally.

Moreover, the characteristics of cyberspace make national and international laws inappropriate to keep with the digital developments. So, governments themselves are unable to regulate the cyberspace activities because the mechanism by which laws are adopted does not match the ubiquitous nature of cyberspace activities. Also, it becomes almost difficult to arrive at an international consensus on the need for adopting new rules. This is due to the idea that there is not a unified approach or view towards the nature of cyberspace activities. This calls for the need to adopt new rules and consensus that may govern the cyberspace activities in an effective way internationally.

REFERENCES

Albakjaji, M., Adams, J., Almahmoud, H., & Alshishani, A. (2020). The legal dilemma in governing the privacy right of e-commerce users: Evidence from the USA context. *International Journal of Service Science, Management, Engineering, and Technology (IJSSMET), 12*(3), 1-11.

BBC News. (2019). *Google 'tracking iPhone users' case goes ahead.* Retrieved from

https://www.bbc.com/news/technology-49908606
Bellanger, P. (2011). *From sovereignty in general to digital sovereignty in particular.* Retrieved from http://lecercle.lesechos.fr/entreprises-marches/high-tech-medias/internet/221137239/souverainete-general-et-souverainete-numeriq
Brenkert, G. (2009). Google, human rights and moral compromise. *Journal of Business Ethics, 85*(1), 453-478.
Broersma, M. (2013). *UK users sue Google over safari tracking.* Retrieved from https://www.silicon.co.uk/workspace/google-safari-lawsuit-uk-privacy-tracking-105574
Broersma, M. (2018). *High court blocks mass lawsuit over Google iPhone tracking.* Retrieved from https://www.silicon.co.uk/workspace/high-court-blocks-google-iphone-tracking-lawsuit-237667
Cain, R.M. (2002). Global privacy concerns and regulation: Is the United States a world apart? International Review of Law. *Computers & Technology, 16*(1), 23–34.
Choucri, N., & Clark, D. (2013). Who controls cyberspace? *Bulletin of the Atomic Scientists, 69*(5), 21-31.
Couture, S., & Toupin, S. (2019). What does the notion of sovereignty mean when referring to the digital? *New Media & Society*, *21*(10), 2305-2322.
Deibert, R., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war. *Security Dialogue, 43*(1), 3-24.
Demchak, C., & Dombrowski, P. (2014). *Cyber westphalia asserting state prerogatives cyberspace.*
De-Smedt, S., Dekeyser, G., & Couter, Y. (2018). *Owners of Facebook fan pages warned by EU court of justice*. Retrieved from https://www.lexology.com/library/detail.aspx?g=74285e1e-00b2-4ecd-bdbc-9edfc2673bd2
Duarte, M.E. (2017). *Network sovereignty: Building the internet across Indian country*. University of Washington Press. Seattle.
Hartnett, S. (2011). Google and the twisted cyber spy affair: US-Chinese communication in an Age of Globalization. *Quarterly Journal of Speech, 97*(4), 411-434.
Hedley, S. (2003). Nations, markets, and other imaginary places: Who makes the law in cyberspace? *Information & Communications Technology Law, 12*(3), 215-224.
Hongju, K.H. (2012). International law in cyberspace. *Harvard International Law journal*, *54*(1), 1-12.
Kauffma, R., Lee, Y., Prosch, M., & Steinbart, J. (2011). A survey of consumer information privacy from the accounting information systems perspective. *Journal of Information Systems: Fall, 25*(2), 47-79.
Kucklich, J. (2009). Virtual worlds and their discontents precarious sovereignty, governmentality, and the ideology of play. *Games and Culture*, *4*(4), 340-352.
Kulesza, J., & Balleste, R. (2014). Signs and portents in cyberspace: The rise of jus internet as a new order in international law. *St. Thomas University School of Law Legal Studies Research*, *1*(1), 1311-1349.
Lewis, J. (2010). Sovereignty and the role of government in cyberspace. *The Brown Journal of World Affairs, 16*(2), 55-65.
Margulies, P. (2013). Sovereignty and cyberattacks: Technology's challenge to the law of state responsibility. *Melbourne Journal of International Law*, *14*(1), 1-24.
Pardau, S., & Edwards, B. (2017). The FTC, the unfairness doctrine, and privacy by design: New legal frontiers in cyber security. *Journal of Business & Technology Law*, *12*(1), 227-276.
Salinas, S. (2018). Facebook stock slides after FTC launches probe of data scandal. *CNBC News, Published.* Retrieved from https://www.cnbc.com/2018/03/26/ftc-confirms-facebook-data-breach-investigation.html
Schmitt, M. (2013). Reaction cyberspace and international law: The penumbral mist of uncertainty. *Harvard Law Review Forum*, *126*(2), 14-37.
Schneider, G. (2017). *Electronic commerce*. Cengage Learning, Cengage.
Sheldon, J. (2014). Geopolitics and cyber power: Why geography still matters, in American foreign policy interests. *The Journal of the National Committee on American Foreign Policy, 36*(5), 286-293.
Tan, J., & Tan, A. (2012). Business under threat, technology under attack, ethics under fire: The experience of Google in China. *Journal of Business Ethics*, *110*(1), 469-479.
Ziegeldorf, J.H., Morchon O.G., & Wehrle, K. (2014). Privacy in the internet of things: Threats and challenges. *Security and Communication Networks Security Communication Networks*, *7*(1), 2728–2742.