Governance Of Cyberspace: Personal Liberty VS. National Security

Ridoan Karim, Tasmeem Chowdhury Bonhi, Rawnak Afroze

Abstract: The term 'Governance' is defined as structures and processes that are designed to ensure primarily accountability, transparency, rule of law, equity, inclusiveness, empowerment, and broad-based participation. On the other hand, cyberspace is a borderless public space in which individuals communicate and interact, regardless of their citizenship, nationality, ethnicity, political orientation, or gender. Individuals use cyberspace to conduct business, make policies, and organize their private lives. This significant space does not have any common rules, a governance apparatus, or control mechanisms that would protect people's activities. Therefore, this research attempts to clarify the principles of sovereignty, and activities in cyberspace, to help establish a standard governance system within the international regulatory regime. Societies are becoming more dependent on computer networks and vulnerable to cyber-crime and terrorism. Measures to protect information systems have received increasing attention. But there does exist some concerns about the measures; such as: what legal standards should govern the use of these measures? What nontechnical constraints should be placed on them? What importance should be assigned to these constraints in designing/implementing technologically robust solutions? In view of the novel character of cyberspace and the vulnerability of cyber infrastructure there is a noticeable uncertainty among governments and legal scholars as to whether the traditional principles of customary international law are sufficiently apt to provide the desired answers to some worrying questions. The purpose of this paper is to hence shed light on the responses of good governance and cyberspace in the context of international political and legal regime. Based on qualitative methodological framework and utilization of secondary sources, the paper emphasizes on the discussion of personal liberty vs. national security and recommends which approach to follow. This paper thoroughly discusses the rights to privacy, the protections against unwarranted searches and seizures, and the rights to due process of law.

Index Terms: Privacy Governance, Cyberspace, Privacy Protection, Global Cyberspace, National Security.

1. INTRODUCTION

The term governance was coined from the Latin word "gubertnare" and even have known to originate from the Greek word "Kubernaein that means to steer (Plattner, 2013). Therefore, governance indicates to steer, direct or control a state or group of people (Grugel & Piper, 2007). Governance covers the areas of structures, processes, which are devised to ensure transparency, responsibility receptiveness, rule of law, consistency, equality, liberation, and general participation (Kingsbury, Krisch & Stewart 2005). Governance also includes the standards, moral and principles through which public matters are resolved in an impartial way (Nuscheler & Wittmann 2017). Thus, in a broad sense it can be said that governance is about the culture and the established environment where people with different interests interact in various public affairs. Therefore, it is something subtle and may not be clearly noticeable. It can be considered as the most vital organ of the government! Many international organizations; such as the World Bank, UNDP, OECD Development Assistance Committee (DAC) have expressed governance as the power that is exercised to as to control a nation's political, economic and managerial affairs (Nuscheler & Wittmann 2017). Governance has also been observed as a power relationship where official or unofficial procedures are used in devising rules and regulations and to distribute resources. It is mainly a continuous practice of decision making and tool for holding governments responsible for things (EDUCATION: UNESCO).

- *Ridoan Karim is a Lecturer in the School of Business Administration, East Delta University, Chattogram, Bangladesh, PH-+8801676513607. E-mail: ridoan.k@eastdelta.edu.bd*
- *Tasmeem Chowdhury Bonhi is a Lecturer in the School of Business Administration, East Delta University, Chattogram, Bangladesh, E-mail: tasmeem.c@eastdelta.edu.bd*
- *Rawnak Afroze is a Lecturer in the School of Business Administration, East Delta University, Chattogram, Bangladesh, E-mail: rawnak.a@eastdelta.edu.bd*

In a broad sense, there is no fixed description of the word governance and several scholars have defined the term in many ways. In this current era of fast paced globalization, internationalization with lots of uncertainties and insecurities, nations who are developed or even developing are in search for a new way of governance that is suited in the current times. Through this, nations aim to achieve and sustain a good position in mainly in financial competitiveness. Good governance is a popular term used in the development literature where scholars seek to convey the idea that good governance is a necessary pre-requisite for achieving an environment that promotes sustainable human development with significant reduction in poverty (Graham, Plumptre & Amos 2003). One of the primary objectives of the Millennium Development Goals (MDGs) includes good governance (United Nations Millennium Development Goals). According to Nygår (2017), there are eight traits that reflect good governance for a nation that is striving towards sustainable development. The traits include; involvement, consent oriented, transparent, responsible, approachable, operative and competitive, equality and encourages rule of law (Nygård, 2017). However, these traits have been established through the vast literature that is available on governance and in true sense there seems to be no such fixed traits that signify good governance. Good governance should cater to the present and future requirement of the society and the government and should endorse discretion in both decision and policy making. It should take an account of the best interests of all stakeholder (Nygård, 2017).

2 CYBERSPACE AND INTERNATIONAL LAW

International law has defined a state as a territory that comprises a population that is represented by an efficient government body (Gray, 2018). While all three aspects of the state are important – without a government there cannot be a state, and the reason for the state is the well-being of the population – it is arguably the territory that is the single most important delimiting criterion. The territory effectively determines the population, and the most important

demarcation of the government's legitimate power (its jurisdiction) is the territory (Anderson, 2013). This territorial basis for political governance has been put in question by increased travel, migration and economic exchange, and governments now exercise at least some aspects of jurisdiction over considerable numbers of events abroad (Anderson, 2013). However, this complication is minor compared to those caused by the Internet. Even though governments are increasingly taking control over their national cyberspaces, and even though the principle of territoriality provides that a state has jurisdiction over servers and nodes within its recognized borders (Ghappour, 2017), communication between servers and computers is routed in international webs mostly operated by private networks, which are not controlled by any one government, and many virtual national assets are stored in servers abroad. Business offers, opinions and fraudulent messages sent from one country and stored in a server in another country may affect events in a third country. Perhaps most importantly, national assets in cyberspace – public and private – can more or less easily be surveyed, affected or even controlled through cyber operations from foreign states, and in particular from a few very technologically advanced ones. Thus, researchers have come to conclude that the Internet is not under the sole control of governments (Avant, Kahler & Pielemeier, 2017), or even a new dimension, not subject to the same regulation as other spheres of human activities. Nevertheless, the Internet and other computer networks have physical locations, under the jurisdiction of one or more states, and the actors have nationality, regardless of whether they are individuals or corporations (Knoke, 2018). In addition, cyberspace has been securitized, and states seek to protect their critical cyber infrastructure from criminal actors and political enemies. It is therefore only logical that states have proclaimed authority on jurisdiction over computer networks, in an increasingly assertive way (Wrange, 2014). As a further corollary, international law that presently operates, is applicable for computer networks. Excluding the Budapest Convention against Cybercrime, and possibly some provisions in the ITU Convention (drafted long before Internet) (Clough, 2014), there is no international convention on the topic (Ebbesson & Mahmoudi 2014). The UN report (Developments in the field of information and telecommunications with respect to international security) – written by a group of experts -- is the closest thing we have to an authoritative intergovernmental opinion (Ebbesson & Mahmoudi 2014). There are very few instances of opinio juris, very little, if any, confirmed state practice, and no judgments or reports from international adjudicative or monitoring bodies (Ebbesson & Mahmoudi 2014). As mentioned, there is not even very much doctrine; most writers who have engaged in international law aspects of cyber sphere have written about international humanitarian law and its influence so far (Ebbesson & Mahmoudi 2014). One important exception is the Tallinn Manual that was written by a drafted by a unit of professionals at the appeal of the NATO Cooperative Cyber Defense Centre of Excellence and published in 2013, which deals expertly but briefly and not conclusively with some peacetime uses of Internet (Ebbesson & Mahmoudi 2014)..

3 CYBERSPACE AND GOOD GOVERNANCE

Cyberspace is free from any boundary where people regardless of their nationality, ethnicity, political views or sex connect and network. The internet and Cyberspace is a common platform through which people conduct businesses, generate policies and make operate many things in their day to day lives. However, this platform is still not controlled by rules or regulations or any administration that would secure and safeguard individuals' actions. Nonetheless, the International law on Human Rights rules and regulations can help as a guideline or skeleton in preparation of governance norms and standards in the field of cyberspace. Conversely, the nature of the space is such that yet we do not understand the ways to govern it properly. The space is straight forward and clear by its nature, however, it is developed, explained, restricted and expurgated by those who use it. Internet communication is often anonymous and used and shared with the public worldwide, which usually remains unknown to the individual Internet user; namely, each of us (Mihr, 2014). Through new technologies, cyberspace offers an environment that consists of many participants who have the ability to affect and influence each other and thus, governing such space can be very much complex and complicated. We nonetheless share our most private and personal data with this anonymous audience. Today, this global, public community numbers around 2.7 billion Internet users (Digital in 2017: Global Overview). If cyberspace were a country, it would be the largest and most populated in the world, albeit one without any constitutions or government. This "space" has no legislative or otherwise democratic decision-making bodies. It has no police or law enforcement mechanism, let alone protection mechanism to safeguard human rights for all Internet citizens. The main issues for governance in the emerging global information society are 'sovereignty' and 'exercise of jurisdiction'. The transformation of the sovereignty of states resulting from globalization is at the core of the institutional aspects of governance. 'Cyberspace' has been defined as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Computer Security Resource Centre). It is true that cyberspace is characterized by anonymity and ubiquity. Therefore it seems logical to assimilate it to the high seas, international airspace and outer space, i.e., to consider it a 'global common' or legally a res communis omnium (Heinegg, 2012). However, these characterizations merely justify the obvious conclusion that cyberspace in its entirety is not subject to the sovereignty of a single State or of a group of States. In view of its characteristics it is immune from appropriation. Despite of the correct classification of 'cyberspace as such' as a res communis omnium State practice gives sufficient evidence that cyberspace, or rather: components thereof, is not immune from sovereignty and from the exercise of jurisdiction. On the one hand, States have exercised, and will continue to exercise, their criminal jurisdiction vis-à-vis cybercrimes and they continue to regulate activities in cyberspace (Buchan, & Tsagourias 2016). On the other hand, it is important to bear in mind that "cyberspace requires a physical architecture to exist" (Franzese, 2009). The respective equipment is usually located within the territory of a State. It is owned by the government or by corporations. It is connected to the national electric grid. The integration of physical components, i.e., of cyber infrastructure located within a State's territory, into the 'global domain' of cyberspace cannot be interpreted as a waiver of the exercise of territorial

sovereignty (Grooters, 2002). In view of the genuine architecture of cyberspace it may be difficult to exercise sovereignty. Still, the technological and technical problems involved do not prevent a State from exercising its sovereignty, especially its criminal jurisdiction, to the cyber infrastructure located in areas covered by its territorial sovereignty. States have continuously emphasized their right to exercise control over the cyber infrastructure located in their respective territory, to exercise their jurisdiction over cyber activities on their territory, and to protect their cyber infrastructure against any trans-border interference by other States or by individuals (Osula, 2015). However, the problem occurs when states may have many reasons to take measures also in foreign cyberspace. Some of these reasons are legitimate as such, like investigations of and responses to terrorism and other crimes. Others may be more dubious, like intelligence or sabotage. Many such measures are covered by various international conventions against transnational crime and terrorism. While these conventions do not allow intrusions, like unauthorized data access, in the jurisdictions of other states, they do mandate states to cooperate with one another, as does the Council of Europe's Convention on Cybercrime (Broadhurst, 2006). Most States engage in intelligence collection abroad. Although certain activities—including cyber operations—may violate another State's domestic law, there is also a chance that such activities also violate international law. Disrespecting another State's domestic laws can have serious legal and foreign policy consequences. As a legal matter, such an action could result in the criminal prosecution and punishment of a State's agents. From a foreign policy perspective, one can look to the consequences that flow from disclosures related to such programs. But such domestic law and foreign policy issues do not resolve the independent question of whether the activity violates international law. In certain circumstances, one State's non-consensual cyber operation in another State's territory could violate international law, even if it falls below the threshold of a use of force. This is a challenging area of the law that raises difficult questions. The very design of the Internet may lead to some encroachment on other sovereign jurisdictions. It needs to be emphasized that the applicability of the principle of sovereignty, and activities in, cyberspace is not barred by the innovative and novel character of the underlying technology. This holds true for the majority of rules and principles of customary international law that do apply to cyberspace and to cyber activities. This does not necessarily mean that the said rules and principles are applicable to cyberspace in their traditional interpretation. In view of the novel character of cyberspace and in view of the vulnerability of cyber infrastructure and cyber components there is a noticeable uncertainty amongst governments and legal scholars as to whether the traditional rules and principles of customary international law are sufficiently apt to provide the desired answers to some worrying questions. In general, the principle of territorial sovereignty and the ensuing right of a State to exercise its territorial jurisdiction apply to cyberspace insofar as the cyber infrastructure within the territory (or on platforms over which the State exercises exclusive jurisdiction) is concerned. The same holds true for individuals present in that territory or for conduct that either takes place within that territory or that produces (harmful) effects thereon. Scholars also believe that, the exercise of jurisdiction under any of the recognized bases under international law is limited only if there exist explicit rules to that effect (Bederman & Keitner 2016). Therefore, the characteristics of cyberspace pose serious questions and concerns over the exercise of territorial sovereignty and jurisdiction.

4 CIVIL LIBERTIES AND SECURITY IN CYBERSPACE

Societies are becoming more dependent on computer networks, and therefore more vulnerable to cyber-crime and terrorism (Sharma, Mittal & Verma, 2015). Measures to protect information systems have received increasing attention as the threat of attacks grows and the nature of that threat is better understood. However, there remain certain concerns on such measures. They are: what legal standards should govern the use of these measures? What nontechnical constraints are likely to be placed, or should be placed, on them? What importance should be assigned to these constraints in designing and implementing technologically robust solutions and international agreements to facilitate law enforcement? Specific answers to these questions might introduce complex legal and regulatory environment. But certain legal principles are broadly applicable in cyberspace as well, including the right to privacy, the protections against self-incrimination and unwarranted searches and seizures, and the right to due process of law. These civil liberties are supported in international law and guaranteed in varying forms by the national laws and institutions of many countries. An international regime against cyber-crime and terrorism must operate within the constraints of these principles, as defined by the legal frameworks of its States Parties. There is often a tension between protecting civil liberties and enforcing laws to maintain public safety and order. States resolve this tension differently. Agreeing upon a common global level of protection of citizens' rights is problematic due to international variance in normative standards, legal practices, and political objectives. An international common denominator could reduce the level of protections currently afforded in some states to the level of authoritarian states. In the interest of promoting international cooperation and a timely response to the growing threat of cyber-attacks, seeking measures other than agreement on a specific level of protection is more likely to succeed. However, the differences in domestic values and rules may allow misuse of systems set up for preventing, tracking, or punishing cybercrime (Hui, Kim & Wang 2017). Diversion of technologies for illegitimate purposes—such as unwarranted surveillance—is a real threat, especially in countries that give little weight to civil liberty principles constraining such activities (Deflem & McDonough 2015). Countries may be tempted to circumvent legal constraints, moreover, when faced with a national security threat. Systems set up for international cooperation would also introduce new cyber vulnerabilities, as they may be "hacked" or "cracked" and misused by criminals or unauthorized persons. States should address these dangers in the course of developing forms of international cooperation that extend to sharing information and coordinating technology.

4.1 Approaches to Security in Cyberspace

In general, there are two basic approaches to security in cyberspace: a protective one and a reactive one (Drozdova, 2001). Each is constrained in different ways. The protective approach aims to deter criminals through measures that deny access or make a potential target less vulnerable to an attack

(Drozdova, 2001). This approach is focused on defense. It involves designing more secure Internet protocols, introducing trusted routers and virtual private networks, and utilizing firewalls, encryption, automated intrusion detection systems, and other security measures (Kuehl, 2009). The reactive approach, instead, seeks to deter the threat through effective investigation, prosecution, and punishment (Steiner, 2017). Both approaches involve monitoring and diagnosing abnormal and unauthorized activity. The protective approach favors automation as well as oversight and decision-making by computer security experts. The reactive one depends more heavily on the participation of law enforcement and requires end-user-oriented (rather than anonymous) traffic analysis, which may be as intrusive as scanning attached files, keyword searches, and content filtering for signs of potential breaches of criminal law. Real-time investigative capabilities may extend to creating embedded data collection infrastructures and modifying hardware and/or software to provide for confidential law-enforcement access to business, governmental, and private computer networks (Berman, 2017). The two approaches can be complementary. Their relative weights depend on the preferences and capabilities of implementing parties. The protective approach is less intrusive, and it is likely to bring about greater cyber security to its users. However, there are significant obstacles to achieving adequate security (Drozdova, 2001). The reactive approach is inherently more intrusive and more threatening to civil liberties. Nonetheless, it may be more effective in cases of inadequate defense and in safeguarding users who are unable to afford, or unwilling to implement, sufficient protective measures.

4.2 Civil Liberties in Cyberspace

Among the issues considered, privacy in cyberspace is the most controversial and publicly debated. Privacy concerns not only the context of law enforcement, but also day-to-day business practices and an individual's ability to control the treatment of personal data made available in electronic format or accumulated during Internet use. Commercial exploitation of personal data without consent is already leading to enhanced legal protections for privacy (Munir, Yasin & Karim, 2014). The enforcement of such protections will raise the issue of the desirability of using protective versus reactive methods, leading to discussions of what can be done to ensure that any method used will protect privacy interests against unwanted intrusion. Privacy is threatened by businesses and other entities that collect and manipulate personal data, criminals who steal such data or stalk people over the Internet, and governments that pursue surveillance or allow intrusive law-enforcement practices (Tu, 2017). Sophisticated electronic capabilities to collect, analyze, manipulate, and disseminate information, as well as to enable tracking, surveillance, and interference with communications, create unprecedented challenges to privacy. Such technologies are becoming more effective, available, and affordable internationally. At the same time, globalization and growing dependence on information technology in all spheres of society have led to a dramatic increase in the level of electronically compiled and transmitted personal data. The differences in domestic legal standards and practices also endanger private data transmitted over international networks. Even if one state has robust privacy laws, it cannot currently guarantee equivalent levels of protection once the data flow beyond its borders (Weber, 2010). Gaps in protection will be created to the extent that laws and law enforcement fail to keep up with technological capabilities and international discrepancies undermine domestic levels of protection. In comparison with data protection, constraints on police behavior in cyberspace have received far less public attention than privacy problems. This is partly because they are narrowly focused on criminal investigation— while privacy interests span personal, commercial, and government realms—and partly because what is necessary and legally permissible in cyber-related investigation and prosecution procedures is still being determined. The protections against self-incrimination and unwarranted searches and seizures and the rights to due process of law apply in cyberspace as anywhere else. However, technological realities can complicate the observance of these rights. Pursuit of crimes committed over international computer networks is also complicated by the differences in domestic procedures and the absence of a system of international criminal law. International human rights' agreements and many national constitution's guarantee equal and proper treatment of individuals before the law. This guarantee entitles individuals to protection against self-incrimination and arbitrary arrest, detention, or exile. If arrested, one must be informed at the time of arrest of the reasons for the arrest and the charges made. The Universal Declaration of Human Rights and the International Covenant of Civil and Political Rights entitle every person to a fair and public hearing by a competent, independent, and impartial tribunal, in the determination of the person's rights and obligations and of any criminal charge (Donnelly, 2013). Moreover, everyone charged with a penal offense has the right to be presumed innocent until proved guilty according to law in a public trial and the right to call and confront witnesses and to introduce evidence. No one may be found guilty of any penal offense that did not constitute a penal offense under national or international law at the time it was committed, nor may a heavier penalty be imposed than the one applicable at the time the penal offense was committed (Dwivedi, 2017).

4.3 Personal Liberty VS National Security: Which Approach To Follow?

The extent to which the rights to privacy, the protections against unwarranted searches and seizures, and the rights to due process of law constrain an international regime against cyber-crime and terrorism depends on the regime and the domestic laws of participating states (Cuéllar, 2001). National laws often contain exceptions or special privileges for law enforcement to pursue criminal investigations. States have different attitudes toward privacy, law enforcement powers, and due process. However, unilateral responses to cybercrime are not likely to be effective. Confronted with the need for international cooperation, states will look for ways to reconcile these differences or attempt to justify some inappropriate behavior. Greater emphasis on protective technological and legal measures will help reduce the latter outcome. Overall, protective measures, which aim to reduce cyber vulnerabilities and rely on computer security staff for initial reaction to incidents, are less intrusive than measures designed to allow extensive law enforcement presence in cyberspace. The protective approach can be implemented through encryption, automation, and anonymous tagging and tracking—recording fields in packet header information, for example, which does not intrude on the content of messages, or router-assisted fingerprinting of packets without disclosure of their originator

unless sufficient evidence of crime emerges (Clough, 2015). Although better measures will need to be designed and updated continuously to keep up with offenses, this approach can afford greater protection against both cyber-crime and intrusive law enforcement. The reactive approach necessarily involves the participation of law-enforcement officials, who will likely scan files, review content, and engage in other surveillance of communications to collect evidence and to identify perpetrators (Steiner, 2017). Engaging in such activities on a wide "preventive" scale, rather than in targeted and warranted investigations, would raise legal and moral concerns of unduly intrusive policing. Furthermore, even in specific cases of suspected crime, limiting the scope of targeted surveillance may be technologically and operationally difficult. This approach places communications of innocent people and their private information at risk. The reactive approach requires greater scrutiny. While clearly threatening to civil liberties, reactive measures would not necessarily result in fewer crimes and better law enforcement. Even in most technologically and economically developed countries today, police lack equipment and training to meet the growing challenge of the electronic dimensions of crime. Technical experts agree that greater automation is crucial for a timely, scalable, and less intrusive response to international cyber-crime. This offers hope that—in the name of both efficiency and civil liberties—relatively nonintrusive technological measures will be developed and implemented in the near future. Such solutions should provide a more suitable balance among security, law enforcement, and civil liberties in cyberspace. Reactive measures will also be enhanced, however, and will need to be fashioned and monitored to ensure adequate protection of human rights.

5 RECOOMENDATIONS AND CONCLUSIONS

a) Counter-crime and -terrorism measures that take effect on foreign territory will therefore ideally be carried out in cooperation with local law enforcement officers under a convention or through an ad hoc agreement. However, such cooperation cannot always be secured. Therefore, a state may feel tempted to carry out law enforcement or counter-terrorism without proper authorization from the other state concerned. This could involve search of information on private computers in order to prevent or investigate crimes and terrorism; an interdiction of a cyber-attack or a 'hack-back" in real time; or an attack aimed at deterring counter-strikes. It is almost utmost importance that States not only agree on the principal application of customary international law to cyberspace but also on a common interpretation that takes into due consideration the "unique attributes of networked technology" (Heintschel, 2013). Hence it is necessary that governments "continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace" (Mueller, Mathiason & Klein, 2007).

b) The technologies of crime and punishment are undergoing a rapid and profound evolution. Such technologies constitute a moving target for evaluation. However, the legal and normative principles discussed here will endure, because they are independent of specific technological means. As such, they can provide a framework for building a global infrastructure and policy environment that balances the needs for crime-free business, government, and personal communications with the protection of property, privacy, and civil liberties.

c) Where trade-offs between security and civil liberties are required, these trade-offs should be carefully examined with the awareness of threats and social implications of measures against cyber-crime and terrorism. Ensuring the protection of fundamental rights to privacy and due process of law is essential. Such protections should be prominent among the design criteria for technological, policy, and legal measures and should be enforced by law and strong economic and political incentives.

d) Governments value liberty, privacy, and security differently. National rules concerning the intrusiveness of law enforcement, protection of citizens' rights, and international cooperation reflect the country's normative choices about the roles of the state, market, and individual. Comprising the basis of domestic law, these norms affect the international behavior of nation-states. An international regime can help influence these norms over time. Today, when an international regime to combat cyber-crime and terrorism is becoming a reality, there is a special opportunity to promote greater respect for human rights. At the very least, methods for international technological and legal cooperation against cyber-crime and terrorism should not be permitted to become a vehicle for governments to oppress society.

5 REFERENCES

[1] Avant, D., Kahler, M., & Pielemeier, J. (2017). Innovations in Global Governance: How Resilient, How Influential?. Innovations in Global Governance, 1.

[2] Anderson, M. (2013). Frontiers: territory and state formation in the modern world. John Wiley & Sons.

[3] Buchan, R., & Tsagourias, N. (2016). Special Issue: Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence. Journal of Conflict and Security Law, 21(3), 377-381.

[4] Bederman, D., & Keitner, C. (2016). International law frameworks. West Academic.

[5] Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies & Management, 29(3), 408-433.

[6] Berman, P. S. (Ed.). (2017). Law and society approaches to cyberspace. Routledge.

[7] Computer Security Resource Centre. Retrieved March 10, 2018, from https://csrc.nist.gov/Glossary/?term=3818

[8] Cuéllar, M. F. (2001). The transnational dimension of cyber crime and terrorism. Hoover Institution Press.

[9] Clough, J. (2015). Principles of cybercrime. Cambridge University Press.

[10] Clough, J. (2014). A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation. Monash UL Rev., 40, 698.

[11] Donnelly, J. (2013). Universal human rights in theory and practice. Cornell University Press.

[12] Dwivedi, K. (2017). HUMAN RIGHTS PERSPECTIVE IN INDIAN. International Education and Research Journal, 3(5).

[13] Deflem, M., & McDonough, S. (2015). The fear of counterterrorism: surveillance and civil liberties since 9/11. Society, 52(1), 70-79.

[14] Drozdova, E. A. (2001). Civil liberties and security in cyberspace (pp. 183-220). Center for International Security and Cooperation, Stanford University.
[15] Digital in 2017: Global Overview. (n.d.). Retrieved March 10, 2018, from https://wearesocial.com/special-reports/digital-in-2017-global-overview
[16] Drozdova, E. A. (2001). Civil liberties and security in cyberspace (pp. 183-220). Center for International Security and Cooperation, Stanford University.
[17] EDUCATION: UNESCO. (n.d.). Retrieved March 09, 2018, from http://www.unesco.org/new/en/education/themes/strengthening-education-systems/quality-framework/technical-notes/concept-of-governance/
[18] Ebbesson, J., & Mahmoudi, S. (2014). International law and changing perceptions of security: liber amicorum Said Mahmoudi. Leiden: Brill Nijhoff.
[19] Franzese, P. W. (2009). Sovereignty in Cyberspace: Can it exist. AFL rev., 64, 1.
[20] Gray, C. (2018). International law and the use of force. Oxford University Press.
[21] Ghappour, A. (2017). Searching places unknown: law enforcement jurisdiction on the dark web. Stan. L. Rev., 69, 1075.
[22] Graham, J., Plumptre, T. W., & Amos, B. (2003). Principles for good governance in the 21st century. Ottawa: Institute on governance.
[23] Grooters, H. J. (2002). Territorial Jurisdiction in Cyberspace. Or. Rev. Int'l L., 4, 3.
[24] Grugel, J., & Piper, N. (2007). Critical perspectives on global governance: Rights and regulation in governing regimes. Routledge.
[25] Heintschel von Heinegg, W. (2013). Territorial sovereignty and neutrality in cyberspace. International Law Studies, 89(1), 17.
[26] Heinegg, W. H. (2012, June). Legal implications of territorial sovereignty in cyberspace. In Cyber Conflict (CYCON), 2012 4th International Conference on (pp. 1-13). IEEE.
[27] Hui, K. L., Kim, S. H., & Wang, Q. H. (2017). Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. Mis Quarterly, 41(2), 497.
[28] Knoke, D. (2018). Changing organizations: Business networks in the new political economy. Routledge.
[29] Kingsbury, B., Krisch, N., & Stewart, R. B. (2005). The emergence of global administrative law. Law and contemporary problems, 68(3/4), 15-61.
[30] Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. Cyberpower and national security, 24-42.
[31] Mueller, M., Mathiason, J., & Klein, H. (2007). The Internet and global governance: Principles and norms for a new regime. Global Governance: A Review of Multilateralism and International Organizations, 13(2), 237-254.
[32] Mihr, A. (2014). Good cyber governance: The human rights and multi-stakeholder approach. Georgetown Journal of International Affairs, 24-34.
[33] Munir, A. B., Yasin, S. H. M., & Karim, M. E. (2014). Data protection law in Asia. Sweet et Maxwell.
[34] Nuscheler, F., & Wittmann, V. (2017). From governance to good governance. Sustainable Development Policy: A European Perspective, 91.
[35] Nygård, H. M. (2017). Achieving the sustainable development agenda: The governance–conflict nexus. International Area Studies Review, 20(1), 3-18.
[36] Osula, A. M. (2015). Transborder access and territorial sovereignty. Computer Law & Security Review, 31(6), 719-735.
[37] Plattner, M. F. (2013). Reflections on" Governance". Journal of Democracy, 24(4), 17-28.
[38] Sharma, M., Mittal, S., & Verma, A. (2015). Cyber Ethics in Security Application in the Modern Era of Internet. IITM Journal of Management and IT, 6(1), 140-143.
[39] Steiner, H. (2017). Cyber operations, legal rules and state practice: authority and control in international humanitarian law.
[40] Steiner, H. (2017). Cyber operations, legal rules and state practice: authority and control in international humanitarian law.
[41] Tu, R. (2017). Privacy Protection System and Big Data.
[42] United Nations Millennium Development Goals. (n.d.). Retrieved March 09, 2018, from http://www.un.org/millenniumgoals/bkgd.shtml
[43] Wrange, P. (2014). Intervention in national and private cyberspace and international law.
[44] Weber, R. H. (2010). Internet of Things–New security and privacy challenges. Computer law & security review, 26(1), 23-30.