CYBER GOOD GOVERNANCE: A NEW CHALLENGE IN INTERNATIONAL POWER POLITICS?

Nezir Akyeşilmen[♣]

Abstract

This article attempts to analyze processes, discussions and institutions of cyber good governance. Cyber governance is literally, search for a free and safe cyberspace, yet it has become a source of political struggle in International politics. Cyber good governance is a component of global good governance, because cyberspace is global phenomenon. Yet, unlike physical world cyberspace is much complicated and anarchic. It also lacks governing institutions that mitigate anarchy at the global level such as international law, international organizations, great powers and diplomacy. There are some attempts to have governing and regulating institutions in cyberspace but there are several structural, political and technical problems. Central question in cyber governance is who is going to govern it? More importantly, is cyberspace governable?

Key Word: Cyberspace, Cyber Governance, Cybersecurity, Cyber Law.

Introduction

Cyberspace has become a part of our daily life in the last two decades. It encompasses every aspect of our lives with its social, economic, cultural and political dimensions. Despite the numerous benefits and comfort that digitalization provides us with, it also carries serious vital risks and threats. In order to protect against the threats arising from this domain, a number of mechanisms have been developed at individual, social and national levels and measures have been taken. Some of them are are cybersecurity measures and training, digital citizenship education and national cyber security strategy documents. However, since cyberspace is a global network, for a safe cyberspace global measures are required.

Global good governance can be defined as a set of norms, rules, and institutions that consist of minimizing the common benefits and minimizing threats by cooperating with stakeholders such as states, international organizations, corporations, civil society and experts to ensure

♣ Assoc.Prof.Dr., Department of International relationsat Selcuk University. Can be reached via twitter @nezmen

security and sustainable cyberspace. Cyber governance is a component of global good governance. Therefore, it would be more accurate to call it as cyber good governance. In this context, the Council of Europe Cyber Governance Strategy lists the aims of cyber governance as to respect the principles of human rights and the rule of law. The strategic goals are to build online democracy, protect internet users, and ensure respect for online human rights (CoE, 2016: 8).

Cyber good governance is an important and new component of global good governance. But some ambitious stakeholders, especially states, who want to make cyberspace not a cooperation but a platform of conflict and power politics, try to understand and acquire something very different from cyber governance. Those who dominate data in the digital age, will dominate the world. Therefore, there is a global competition for cyber governance, especially among great cyber powers in international relations. There's a big struggle behind the codes. As a matter of fact, they are all about code policies. Basic question is: Who will govern cyberspace? Even more importantly, is cyberspace governable?[1]

Cyber good governance deals with an invisible structure. Unlike the physical world, cyberspace is far more complex, anarchic and lack of governance institutions. To govern the cyberspace, there is little or no international institutions that mitigate anarchy at the global level such as international law, international organizations, great powers and diplomacy. There are some initiatives to create governance institutions and regulatory principles in cyberspace, but there is not a concrete consequence yet. To understand and analyze cyber governance, we need to know how cyber space is. In this context, answers to a wide range of questions will be sought in this work. What are the main features of cyberspace? How is the structure? Who controls the infrastructure of the cyber domain? What are the approaches and mechanisms of cyber governance? What is the main function of cyber governance? Why are some great powers unwilling to make an international cyber treaty?

Cyber Governance as a New Challenge in International Politics

[1] The early version of this article was presented at the **International Conference on Modern Governance**, Organized by Chinese Council for Foreign Affairs, Hangzhou, May 15th -17nd 2018 and also published as a chapter in Akyeşilmen, N.(2018). *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik.*Ankara:Orion kitapevi.

It is an undisputed fact that cyber governance has become an important international issue in international agenda among great powers in recent years. This problem is double-sided. On the one hand, cyber governance is part of global good governance. In other words, it has been a new and big discussion topic for global governance. Jayawardane et al. (2015: 3) argue that cyberspace affects global social and economic relations in the 21st century. It is an integral component of the critical infrastructure in which modern societies are connected and revolutionized communication and socialization. Cyberspace governance is therefore an indispensable element of global governance and is a test area for new models of cooperation that can be adapted to effective governance in other areas. But on the other hand, we have a problem with cyberspace governance. Who's running it? Or who should govern? Perhaps the more vital question is; Can it be governed? In other words, is it possible for people to govern cyberspace? Therefore, when it comes to cyber governance, we face problems within the problem.

Cyber governance means different things for different sectors and different actors. Some see it as a technical problem, others as socio-political one. Some see it as a problem for governments, while others consider it a problem of all stake-holders. All these approaches have their truths, but are they sufficient for explaining the processes and structures? Do they solve the problem of cyber governance?

Initially, discussions on the subject were limited to the Internet. However, it was later understood that cyberspace was a broader, more comprehensive and appropriate concept than the Internet. Thus, in today's literature, the concept of cyberspace is preferred in the literature. Cyber governance is comprehensive, complicated, and complex, since it includes many issues, actors, mechanisms, procedures and tools (Kurbalija, 2016: 16). While there is no consensus on many concepts related to cyberspace, we are faced with new terms and new paradigms every day and every time. Cyber governance is one of the newly emerging concepts in the discipline. Therefore, it is a complex new area that requires conceptual mapping and classification. Or a working definition. Its complexity is related to its multidisciplinary structure that encompasses various aspects such as technology, socio-economics, development, law and politics (Kurbalija, 2016: 28).

There is no widely accepted definition for cyber governance in the literature. The Internet Governance Working Group (WGIG) defined it as follow: Internet governance is the

development and implementation of governments, the private sector and civil society's own roles, common principles, norms, rules, decisions, procedures and programs that shape the development and use of the Internet(Bossey, 2005: 4). This definitions lacks some important features of cyberspace. First of all, it focuses on the internet, which is only one component of cyberspace. However, cyberspace has four different components: User/People, information, logcal framework and physical infrastructure (Pathfinder, 2011: 2). Majority of definitions ignore the user, an important and an active actor of cyberspace.

Cyber space is a unique structure. Therefore, the concepts and theories we use in the physical world or in the traditional sense may be inadequate to understand and explain it. In fact, Jayawardane says that cyber governance is rather complex and difficult. First of all cyberspace has a decentralized structure under the hegemony of the private sector. Yet increasing interest of the state and civil society in recent years has forced a state-centric and a rigit traditional global governance (Jayawardane, 2015: 4). But we will try to understand and make sense of them by establishing analogies with traditional phenomena (since human beings and especially languages are limited phenomenon, since there are no other concepts, theories and instruments). In time, researches, concepts and theories in this direction will develop, and perhaps the concept and theory gap that we face today will be overcome.

First of all, it is useful to look at the concepts of government and governance. According to Farenfest, government is the function of management. Management is to have control over ourselves. Governance is a set of decisions and processes that reflect social expectations through government leadership or management (in the Liberal democratic ideal, we the people rule ourselves)(Farenfest, 2010: 771). In this respect, it expresses a democratic government. In fact, governance envisages a more participatory, egalitarian, and horizontal relationship between stakeholders than the democratic structures that is being applied today. Because, while democracy offers a governing framework that expresses a vertical relationship, governance provides for equal and horizontal participation of stakeholders.

While the concept of governance enshrines the equal participation of different stakeholders at its core, most of the states (those who are truly undemocratic and those who do not care about equal participation on a global scale) consider it a participatory governance rather than

governing from the top. However, cyberspace is a multi-centered, global and anarchic structure beyond the control of states. Trying to control it, targeting to manage instead of governance can ultimately lead us to cyber governance problem. The concept of governance encompasses the norms and rules governing any activity of human beings. It is a set of formal and informal rules applied to social activities such as internet governance, political governance or market governance. Governance is something different from management that includes the formal internal processes of state institutions. Referring to Keohane and Nye Wilson refers to governance as follows: formal and informal institutions and processes that regulate the collective actions of a group. The government is a sub-group that forms formal obligations and acts with authority. Governance cannot be applied only by the government. Private companies, professional associations and NGOs are involved in governance without governmental bodies, sometimes together with government bodies (Adams et al., 2015: 26-27; Wilson, 2005: 31-32). It is clear from this definition that governance is beyond the conceptof management or governing.

Cyber governance includes formal and informal legal mechanisms, rules and policies that regulate the transnational actions and behaviors of state and non-governmental stakeholders to ensure data integrity according to Almeida (Almeida, 2016). ISACA, on the other hand, participates in discussion with information security governance and defines a structure as a system for managing and guiding information security (ISACA, 2014: 3).

Anarchic Cyber Space Governance: A Story of an Oksimoron?

Cyber space began to affect all aspects of our daily lives: from trade to energy, from communication to finance, transportation and entertainment. It provides us with a number of benefits, but it also includes some risks and threats. Today, cyber security has become one of the most important issues of human, national and international security agenda. Today, many smart tools and equipment make our lives easier. Internet of Things (IoTs), big data, block chain technology and artificial intelligence will further digitize our lives in the near future. In 2020, it is estimated that billions of devices will be connected to the internet. Big data will increase scientific research and technological innovations. Some statistics about the internet show that this structure is enormous and widespread even today.

Bing open, transparent and established as an information-sharing platform cyberspace was exposed to malware, attack and security problems in the early 1980s. Since the emergence of the Elk Cloner (first computer virus) in 1982, the types and concepts of cyber security-related programs have increased dangerously (Landesman, 2011). More than 30% of computers in the world are exposed to malware and cyber attacks (Mello, 2014). There are numerous malware and cyber attacks with different effects on computers and users. According to Green and Rossini (2011), cyber attacks cover a wide range of "cyber security threats, computer viruses, spam, credentials, data breaches, service slowdowns, and unplanned cybercrime."

Cyber threats are not limited to malwares, but also include social engineering and physical attacks. The targets of these aggressors can be individuals and private companies, government agencies and infrastructure services such as energy, transport, finance and communication: “As in traditional warfare, indirect and non-military objectives, such as state institutions, financial institutions, national energy, transport infrastructure and community morale are the main targets of cyber warfare” (Cornish, 2016: 10). Unlike physical spaces, the ever-expanding and growing cyberspace is a man-made, but virtual world that cannot be controlled or constrained by any power. It is very similar to the anarchic environment defined by the "International Relations Theory", in which there is no superior authority. This state of anarchy is even more evident in cyberspace.

In spite of all these, the fact that cyberspace has an anarchic nature does not mean that it is chaotic and that it is devoid of rules and norms. There are some technical and political organizations that regulate this anarchic structure, albeit weakly. Similar to the physical spaces, it is possible to talk about a number of regulatory bodies and rules such as international law, international organizations, great powers, diplomacy, international regimes and universal norms in physical international relations (Bauer, 2007: 1).

Cyberspace is a domain developed and operated mainly by private companies (Wu, 213: 1-6). States are too late to intervene in this sphere (Clark, 2010: 1) and therefore cyberspace is not a state-centric space, but a stakeholder-centered structure. For this reason, states need support and cooperation for a safer cyber compromise with non-state actors such as international organizations, private companies, civil society and even individuals. In other words, cyber governance is only possible through the cooperation of all stakeholders in cyberspace.

What makes the governance difficult in cyberspace is not just the anarchic structure of the system. At the same time, its complexity, global structure and the existence of different actors with different interests and perspectives also complicate the situation. Cyber governance is weak because the number and type of actors involved is high, differences in understanding between actors are huge, and cyberspace is too complex.

Today, cyber space governance is mainly concentrated in a technical field, but in recent years, some states aim to control this domain and thus to increase their international political power. Therefore, international cyber governance is being discussed in international platforms as a political problem in recent years.

The existing governance design or mechanism is based on the Internet Engineering Task Force (IETF), which was established by experts. The Domain Name System (DNS) was established in order to provide names and numbers from the Internet in the 1980s (Knake, 2010: 6). The IP address deployment was also distributed by the IANA Internet Encryption Center (ICANN, 2011,6). Later this task was transferred to ICANN. There are a number of similar institutions and organizations for the operation of the technical infrastructure and the operation of the global network. However, it is the most effective organization that performs a series of functions, the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is responsible for coordinating the technical aspects of DNS. The ICANN archive (2018) describes the organization and its structure as follows:

> *Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization that is organized internationally responsible for Internet Protocol (IP) address space allocation, protocol handle assignment, general (gTLD), and country code (ccTLD) Top Level domain name system management and root server system management functions. These services were first carried out by the Internet Assigned Numbers Authority (IANA) and other agencies as per the agreement with the US government. Today ICANN realizes the function of IANA. As a private-to-public partnership, ICANN works to protect the stability of the Internet's work, to promote competition, to promote the representation of global Internet communities with greater participation, and to develop policies based on grassroots.*

In recent years, states have launched international initiatives at the international level to deal with the threats generated by cyberspace, to increase their power in this area and to become a partner in global internet governance. These efforts are continuing today. On the one hand, the literature in this field is developing rapidly and the theoretical discussions are also concentrated.

Approaches to Cyber Governance s

Governance issues in cyberspace consist of technical and political components. Other than technical aspects such as domain names, root servers, internet protocols and IP numbers, global routing and maintenance, cyber governance covers digitalizing socio-politics such as online freedom, privacy, e-economy and e-commerce regulation, IoTs, big data, block chain and cloud technology issues and cybersecurity that includes all.

There are different views and approaches to the scope, nature and limitations of cyber governance. For example, a narrow and broad approach; a technical and a political approach; decentralized and centralized approaches. Each of these approaches has different views, explanations and solutions for the cyber governance.

Technical and Narrow Approach

The technical and narrow approach is close insights that focus on the technical infrastructure of cyberspace. In particular, internet layers, internet protocols, TCP/IP, root servers, Domain Name System (DNS), Internet Names and Numbers Allocation Systems (ICANN). According to this view, cyber governance is a technical issue that should be carried out by technical experts (Kurbalija, 2016: 15). They want internet to remain as a more free and flexible structure, which does not want to put it under the control of politics. They think that if the political mechanisms come into play, the internet will suffer more. They consider that technical staff and structures should be decisive and effective in governance as they consider it a technical domain.

Political and Broad Approach

The broad approach views cyber governance as a social and political process. According to this view, cyber governance should go beyond the technical infrastructure and include social, economic, cultural, legal and political issues. Therefore, the governance process must go

beyond the technical community, including other stakeholders such as civil society, companies and governments (Kurbalija, 2016: 15).

There are also centralized and decentralized approaches to the broader approach and with different views on governance. While the central approach envisages a centralized management process, the decentralized view reveals the decentralized nature of the internet and argues that cyber governance should be removed from a central government. Centralized approach claims that the concept of governance is related to government. For this reason, governments should manage cyberspace. Other actors can only assist the government. Equal participatory engagement cannot be considered. They foresee a more state-centric understanding.

On the other hand, there is a view that cyberspace is not a state centered domain. They argue that cyberspace is a multi-stakeholder field, that each stakeholder's destructive power is close to each other, and that all can be made more secure by co-operation with common governance. Private companies and non-state actors are the central players in this domain (Akyeşilmen, 2016: 41-46). Therefore, cyberspace must be managed by all stakeholders, including states, international organizations, private companies, civil society representatives and even individuals. Jayawardane and others support this approach: "Cyberspace governance is complex and controversial. The decentralized nature of the environment which is largely owned by the private sector and operated by the private companies, but which attracts and concerns governments and civil society, challenges traditional methods of global governance that tend to be state-centered and inflexible" (2015: 4).

The Internet Governance Working Group Report (WGIG) sets out four key public policy areas that provide a holistic approach to cyber governance:

> *(a) Issues related to governing of infrastructure and critical internet resources,* domain name system and *management of internet protocol addresses (IP addresses), root server system management, technical standards, infrastructure connections, telecommunication infrastructure, innovation and convergence technologies as well as multilingualism. These issues are directly related to internet governance and are within the limits of existing organizations responsible for them; (b) Internet, spam, network security and cybercrime issues. While these issues are directly related to internet governance, the quality of global cooperation is not well defined; (c) issues that are*

relevant to the Internet, but which have far more influence than the Internet and which are responsible for existing organizations such as intellectual property rights or international trade; (d) Issues relating to the development aspects of Internet governance, particularly capacity building in developing countries (Bossey, 2005: 5).

Based on these analyzes, a desired model for cyber governance can be summarized as follows:

- An inclusive and holistic approach to governance is necessary. It should therefore be a multi-stakeholder system that envisages the participation of states, international organizations, the private sector, civil society and technical community.
- The Internet is built on the principle of transparency, so it should be managed with transparency.
- The management system should strengthen all stakeholders.
- It also needs a fair participation.

However, such models and mechanisms alone cannot provide a safe and free cyberspace. Therefore, comprehensive regulatory mechanisms including norms, regulations, regimes, and processes laid down by all stakeholders should be developed. The sector should go beyond pactophobia (only those that link states) and new laws and international agreements that encourage cooperation and facilitate governance should be made. The numbers of agreements such as the Budapest Convention on Cybercrime by the Council of Europe (CoE) need to be increased. Governments and other stakeholders should be ready to take more responsiblity in cyberspace (Jayawardane et al., 2015: 4-14). These are only possible through the establishment of a comprehensive, holistic, coherent and functioning cyber governance mechanism.

International Law as an Instituton of Cyber Governance: Is Regime Theory an Answer?

Every aspect of cyberspace governance has a legal dimension. But because the law is progressing at a much lower rate than technology, cyber law, especially cyber international law, is still at its infancy level.

There are two different views on how to organize the cyberspace through (inter)national law. First, there are those who argue that cyberspace is not a different sphere i.e. it is continuation of physical spaces and therefore should be governed by existing international legal regulations instead of a new one. There are also those who claim that cyberspace is different from the physical spaces and requires a new legal order (Kurbalija, 2014: 85). At present, the states maintain their dominance in the first approach, as the states do not agree cooperation in this field. International problems encountered in the cyber domain are tried to be solved by the current international legal norms, but there are doubts that they are often effective and efficient. This is an important weakness of this approach.

One of the main features of the international structure is that it is based on the physical boundaries and jurisdiction of the state. However, although it is decentralized and anarchic, cyberspace has no boundaries. Therefore, states have no clear jurisdiction (strong legal sanctions), and a single actor is not predominant at the system level. Again, many private actors are stronger than many states in terms of governing and manipulating cyberspace. In addition, many individual hackers can launch devastating attacks such as states and/or companies. Therefore, unlike the physical world, there are many more equivalent actors or stakeholders in the cyber world.

There are regimes that regulate special issues in international relations such as trade, environment, human rights etc. Within the framework of international agreements, norms, standards and institutions developed on the basis of cooperation of states on certain issues or problematic ares in global or regional scale are organized and managed (Verbeek, 2011). Cyberspace also requires global cooperation, agreements, and legal arrangements, because of its global and anarchic nature, connecting all people, and the large number of benefits it provides, as well as numerous global threats it poses. More importantly, it is clear that cooperation and regulation limited to traditional state-centric or states is not sufficient. But to date, the international community has not been able to make a promising effort to establish a safe cyberspace and to protect global interests in the sphere of cyber governance.

Comprehensive work on the cybercrime of the UN Crime and Drug Office -UNODC Expert Group, in addition to some regional initiatives such as the Council of Europe Cybercrime Convention, OECD Online Identity Theft Guidelines, Shanghai Cooperation Organization's Information Security Cooperation, EU Cyber Attacks Directive and the African Union Cyber

Security and Protection of Personal Data Convention. (2013); and Cyber Security, which was adopted by ITU in 2007, has no international law regulation other than the Global Cyber Security Agenda among Member States (Coe, 2001). There have been some initiatives initiated by Russia and China at the UN level for cybersecurity cooperation, but so far no concrete results have been received. There are a number of soft law regulations in this area, but their effectiveness is seriously questioned. In short, despite these weak efforts, it is understood that there is a reluctance to make a comprehensive international agreement or to establish a regime in cyberspace at the international level.

Why is that so? Who is avoiding collaboration? Who does not want an international cooperation? How effective is a legal regulation limited to states?

The state is a late comer in cyberspace, but due to its power of regulation(making international treaties) and sovereignty tries to increase its power, has tried to control other stakeholders in cyberspace. However the power, interests, relations and threats to each country are different in cyberspace and thus their policies towards this domain differ. This short discussion will focus on the policies of the US and its allies representing the status quo and the policies of other countries led by Russia and China, which are developing moves against it.

Russia and China are making a serious effort to make states control the internet. Due to cyber attacks, cyber intelligence, cybercrime and cyber conflicts, this idea is attractive to many countries (Knake, 2010: 3). They want to have a say in cyberspace governance, which plays an important role in the economic and social development of many digitalized countries, including China and Russian Federation. All countries, especially China and Russia, are particularly interested in the ICANN administration in cyber governance where the US is active (Yan, 2015: 5) and dominent.

The international cyber governance policies of the US and its allies seem to be a one-sided game. Although the Internet is an ARPANET product, a US government-funded project, it has gone beyond the control of the United States due to its globalized, anarchic structure and multi-actor characteristics. In the United States, the Department of Defense, the NASA, the Ministry of Commerce and the presidential office in recent years are trying to play an active role in internet governance (Kurbalija, 2014: 181-182). The US is in favor of the protection of

the status quo because US-based individuals and NGOs are active in ICANN and other technical governance institutions, even if they are not directly US government agencies. It does not want to share this activity and power with other countries, especially China and Russia, whichit he sees as rivals.

Knake claims the US should develop a relationship based on cooperation with international actors. For this, first of all, it should strive to protect the free internet. Second, it should endeavor to establish an international mechanism for countries to be held accountable for their actions in cyberspace, and finally establish an internal mechanism to follow the cyber agenda. In order to achieve these goals, a multi-dimensional multi-actor cyber governance regime should be established in cooperation with other countries. It should encourage other countries to make arrangements for domestic cyberspace for a safe cyber domain, and finally establish itself in an improved legal system in this field (Knake, 2010: 3-4).

In spite of different approaches and perspectives of global cyber powers, there are some constructive recommendations in the literature and partly in practice. If these suggestions are developed, they may turn into concrete legal texts and legal structures in the future.

Premature Models for Cyber Governance

There are several concrete mechanisms proposed in theory and practice for cyberspace governance, but they are far from responding to the problem adequately. Here the focus will be on two proposals. One is the the regime comples theory proposed by Joseph Nye, the other is the Internet Governance Forum (IGF).

Theory of Regime and Regime Complex

Although the mechanism developed by Nye was based on the complex interdependence theory previously developed by Nye and Keohane. This proposal goes beyond their original theory i.e. it is updated with the name of regime complex theory. Nye's proposed solution for cyber governance is the liberal institutionalism and international regime theory on which he is an expert. The international regime is defined in the literature as acting as a secret coalition between the actors such as states, international organizations, multinational corporations, and so on, with similar understanding of the same procedures and desirable outcomes (Verbeek,

2011: 559). In another definition, according to Stephan Krasner, the regime is the principles, norms, rules and decision-making procedures in which the expectations of the actors in a certain issues in international relations get closer '(Oshiba, 2010: 261).

Nye's suggestion goes far beyond regime theory for cyber governance, because it thinks that cyberspace cannot be ruled by a traditional international regime. He recommends the following regime and regime complex:

> *Regimes are a subset of norms that reveal expectations of appropriate behavior. Norms may be illustrative, prescriptive, or both. They may be institutionalized or not institutionalized at different degrees. There is a degree of hierarchical coherence between the norms of a regime. A regimen complex is a set of loosely coupled regimes. On a formal spectrum of institutionalization, a regime complex is located somewhere between a single legal instrument at one end and a fragmented arrangement on the other. Although there is not a single regime for cyber publicity governance, there are a number of loosely bound norms and institutions in place that can be defined by an integrated organization that imposes regulation through hierarchical rules, and between a core structure and multi-part practices and institutions (2014: 5).*

For the Global Internet Governance Commission (GCIG), which seeks to develop a strategic vision for the stability, security and governance of Cyberspace, J. Nye's report, Regime Complex to Manage Global Cyber Activities (2014), focuses on four key elements:

> *Enhancing governance legitimacy —including regulatory approaches and standards*
> • *Stimulating economic innovation and growth —including critical Internet resources, infrastructure*
> *and competition policy*
> • *Ensuring human rights online —including establishing the principle of technological neutrality*
> *for human rights, privacy and free expression*
> • *Avoiding systemic risk — including establishing norms regarding state conduct, cybercrime. (Nye, 2014: v)*

Nye argues that the regime and regime complex model he develops provides a comprehensive and integrated governance approach. Nye's model also focuses on both technical and political aspects of cyberspace, and finally emphasizes cybersecurity and human rights issues (Nye, 2014: 5). Although he argues that the model he developed provides a good framework, in the

concluding part of the report, he says that "Predicting the future of the normative structures that will govern the various issues of cyberspace is impossible because of the newness and volatility of the technology, the rapid changes in economic and political interests, and the social and generational cognitive evolution that is affecting how state and non-state actors understand and define their interests (Nye, 2014: 15). Thus he admits that his proposal is incomplete. Given the speed and transformation of cyber technology, this analysis by Nye seems to be much more realistic than the cyber governance model it proposes. Like Nye, Almeida also emphasizes that rapid change and transformation in cyber technology makes governance difficult (Aimeida, 2016).

Internet Governance Forum (IGF)

The second model proposed for cyber governance is the Internet Governance Forum (IGF) developed by the United Nations and based on a more loose and multi-stakeholder practice. On its official website, the IGF is defined as a "forum based on a multi-stakeholder dialogue on public policy issues related to the key elements of Internet governance issues, such as the sustainability, security, stability and development of the Internet. The Secretary-General of the United Nations officially announced the establishment of the IGF in July 2006 and held its first meeting in October / November 2006 (UN, 2018).

The IGF stipulates multi-stakeholder and equitable participation. The location and tasks of the IGF are set as a platform for discussions and aim to gather various stakeholder around a table on an egalitarian basis to share knowledge and good practice. IGF develops a common understanding of how to maximize Internet opportunities and address risks and challenges in cyberspace(UN, 2018). The aim of IGF is "to maximize the exchange of ideas on open and inclusive dialogue and issues related to Internet Governance (IG); creating opportunities to share best practices and experiences; identifying emerging problems and bringing them to the attention of relevant institutions and society; to contribute to capacity building for Internet governance" (UN, 2018). IGF organizes seminars, conferences and initiatives at national, regional and international levels to develop the ideas and mechanisms of global cyber governance.

These two models proposed for the governance of cyberspace are recommendations that seek to provide global cyber security and benefits that embrace a holistic approach, including multi-stakeholder, formal and informal norms and procedures. Certainly not the perfect

models, but it seems that they are useful proposal given the current technological developments and the level of global cooperation.

Conclusion

The impact of cyberspace on our daily lives has been deepening day by day in the last thirty years. Critical infrastructures such as rapid development of digitalization in commerce, social life, education, communication, Internet of Things (IoTs), cloud computing, big data and energy, transportation, finance have not only reinforced our lives, but also brought new challenges (ESADE 2018: 7-11).). The transparent nature of cyberspace makes it a clear target for cyber attacks. Anarchic structure has created the problem of cybersecurity and cyber governance. Cyber governance is a new component of global governance.

The decentralized cyberspace system causes a cybersecurity problem. The cybersecurity failure is not only technical, it is also political. In other words, the lack of coherent policies results in cyber insecurity. Thus, there is a need for coherent and stakeholder-based holistic policies, processes, structures, norms and procedures for a free and secure cyberspace. Cybersecurity objectives are the confidentiality, integrity and accessibility of information. It is also an effective refuge for human rights. Cybersecurity failure also leads to a violation of human rights. Therefore, we need a mechanism for safe cyberspace and global good cyber governance for the protection of human rights and creation of free and safe cyberspace.

As seen in the discussions above, for a functioning mechanism, there are some initiatives, but they are far from fulfilling the expectations of humanity. The two proposed models offer a comprehensive and holistic approach that envisages the participation of all stakeholders, including states, private companies, international organizations, civil societies and individuals. However, all the proposed models remain behind because cyber technology is rapidly changing and transforming. Therefore, it is very difficult to predict how a model will handle and improve the problem of cyber governance.

A comprehensive and holistic perspective should be developed to move existing models forward and create a safer cyberspace. A multi-stakeholder model should be envisaged, including states, private companies, international organizations, NGOs, experts and even users. This model should be managed in a transparent manner. The governance model should empower all stakeholders and provide opportunities for their fair participation.

References

Adams, S. ve Diğerleri.(2015). *The Governance of Cybersecurity A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK*.Tilbur:Tilburg University.

Akyeşilmen, N.(2016). Cybersecurity and Human rights: Need Fora New Paradigm? *Cyberpolitik Journal.*Vol.1, No.1.pp.38-61.

Almeida,V.(2016). Cyberspace Governance Concepts and Framework. https://cyber.harvard.edu/~valmeida/pdf/Lecture2.pdf [Erişim Tarihi: 16.08.2018].

Bauer, J.M.(2007). Internet Governance: Theory and First Principles. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=DCEEFD890BC0A019F152C4489FA78F69?doi=10.1.1.113.519&rep=rep1&type=pdf [Erişim Tarihi: 16.08.2018].

Beceni, Yasin.(2008).Siber Uzay Kavramı ve Toplumsal etkileri. http://bilgitoplumuhukuku. blogspot.com.tr/2008/09/bilgi-ve-iletiim-teknolojilerihukuku_8713.html [Erişim tarihi: 01.03.2018].

Choucri, N. and Clark, D. (2012). Integrating Cyberspace and International Relations: The CoEvolution, Boston: MIT Working paper-29.

CoE.(2016).*Internet Governance: Council of Europe Strategy 2016-2019*. https://rm.coe.int/internet-governance-strategy-2016-2019-updated-version-06-mar-2018/1680790ebe [Erişim tarihi: 16.08.2018].

Cyberdefinitions.(2016).Global Cyber definitions Database. http://cyberdefinitions. newamerica.org [Erişim tarihi: 01.03.2018].

Esade.(2018). Global Cyber Governance: Preparing for New Business Risks. http://itemsweb.esade.edu/wi/web/risk-nexus-april-2015-global-cyber-governance.pdf [Erişim tarihi: 13.02.2018].

Farenfest, D.(2010).Government, Governing and Governance.*Critical Sociology.*36(6), ss.771-774. https://www.researchgate.net/publication/254084388_Government_Governing_and_Governance [Erişim Tarihi: 15.08.2018].

Green, N. and Rossini, C.(2011).Cyber Security and Human Rights. available at https://www.gccs2015.com/sites/default/files/documents/Introduction%20Document%20for%20GCCS2015%20Webinar%20Series%20-%20Cybersecurity%20and%20Human%20Rights%20%281%29.pdf [Accessed on 04.03.2018].

ICANN.(2011).Internet Protocol(IP)Addresses. https://www.icann.org/en/system/files/files/ ip-addresses-beginners-guide-04mar11-en.pdf[Erişim tarihi: 17.08.2018].

ICANN.(2018). https://archive.icann.org/tr/turkish.html [Erişim tarihi: 17.08.2018].

IFG.(2018).Internet Governance Forum. https://www.intgovforum.org/multilingual [Erişim tarihi: 04.03.2018].

Internetlivestats.(2018).Internet live stats. http://www.internetlivestats.com[Erişim tarihi: 13.02.2018].

ISACA.(2014).*2014 Governance of Cybersecurity*.Naarden, ISACA.

ISACA.(2016).Cybersecurity Fundemantals Glossary. http://www.isaca.org/ knowledgecenter/ documents/glossary/cybersecurity_fundamentals_glossary. pdf [Erişim tarihi: 13.02.2018].

ITU.(2003). Civil Society Declaration to the World Summit on the Information Society. https://www.itu.int/net/wsis/docs/geneva/civil-society-declaration.pdf [Erişim tarihi: 19.08.2018].

Jayawardane, et.al.(2015).Cyber Governance: Challenges, Solutions and Lessons for Effective Global Governace. http://www.thehagueinstituteforglobaljustice.org/wp-content/uploads/2015/12/ PB17-Cyber-Governance.pdf[Erişim tarihi: 25.02.2018].

Klimburg, A.(2012).National Cybersecurity Framework Manual.Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. Available at https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf [Erişim tarihi: 25.02.2018].

Knake, R.K.(2010).*Internet Governance in an Age of Cyber Insecurity*. https://www.researchgate.net/publication/316040640_Cyberspace_Governance_and_State_Sovereignty[Erişim Tarihi: 17.08.2018].

Kurbalija, J.(2014).Introduction to Internet Governance(6th Edition).Geneva: Diplo Foundation. https://www.diplomacy.edu/sites/default/files/An%20Introduction%20to%20IG_6th%20edition.pdf [Erişim tarihi: 25.02.2018].

Landesman, Mary.(2011).A Brief History of Malware. available at http://antivirus.about.com/od/whatisavirus/a/A-Brief-History-Of-Malware-The-First-25-Years.htm (Last visit: December 1, 2017).

Nye, J.S. (2014). The Regime Complexes for Managing Global Cyber Activities. Boston: J.F. Kennedy School of Government.

Oshiba, R.(2010).Internatiomal Refimes.Government and Politics:Encyclopedia of Life support Sytems .Vol.II.Oxford: Eolss Publishers/UNESCO.ss.260-268.

Osula, A. Roigas, H.(2016).Introduction. in Anna-Maria Osula and Henry Roigas (eds), in International Cyber Norms Legal, Policy & Industry Perspectives, Tallin: NATO Cooperative Cyber Defence Centre of Excellence. available at https://ccdcoe.org/sites/default/files/multimedia/pdf/ InternationalCyberNorms_ full_book.pdf [Erişim tarihi: 25.12.2017].

Pathfinder.(2011).What is cyberspace? examining its components.Pathfinder. Issue no. 153. http://airpower.airforce.gov.au/publications/Details/446/153-What-isCyberspace-Examining-its-Components. aspx [Erişim tarihi: 25.12.2017].

PoKempner, Dinah.(2013).Cyberspace and State Obligations in the Area of Human Rights. in Kathrina Ziolkowski. Peacetime Regime for State Activities in Cyberspace:International Law, International relations and Diplomacy.Talinn: NATO Cooperative Cyber Defence Centre of Excellence.

Verbeek, B.(2011).Regime theory in International Relations. Dowding, *K.Sage Encuclopedia of Power*.Sage.ss.559-562. file:///C:/Users/Dell/Downloads/SageEncyclopediaInternational Regimes%20(2).pdf [Erişim tarihi: 10.09.2018].

Wison, E.(2005). What is Internet Governance and Where Does it Come From?.Int.Pub.Pol.25(1), ss.29-50.

WSIS.(2003).Declaration of Principles for Building the Information Society: a global challenge in the new Millennium. http://www.itu.int/net/wsis/docs/geneva/official/dop.html [Erişim tarihi: 19.08.2018].

Wu, Timothy S.(2013).Cyberspace Sovereignty? - The Internet and the International system. *Harvard Journal of Law and Technology,* Vol.10, no.3.

Yan, L.(2015). Reforming Internet Governance and the Role of China. http://isdp.eu/content/uploads/images/stories/isdp-main-pdf/2015-LiYan-Reforming-Internet-Governance-and-the-role-of-China.pdf[Erişim tarihi: 17.08.2018].