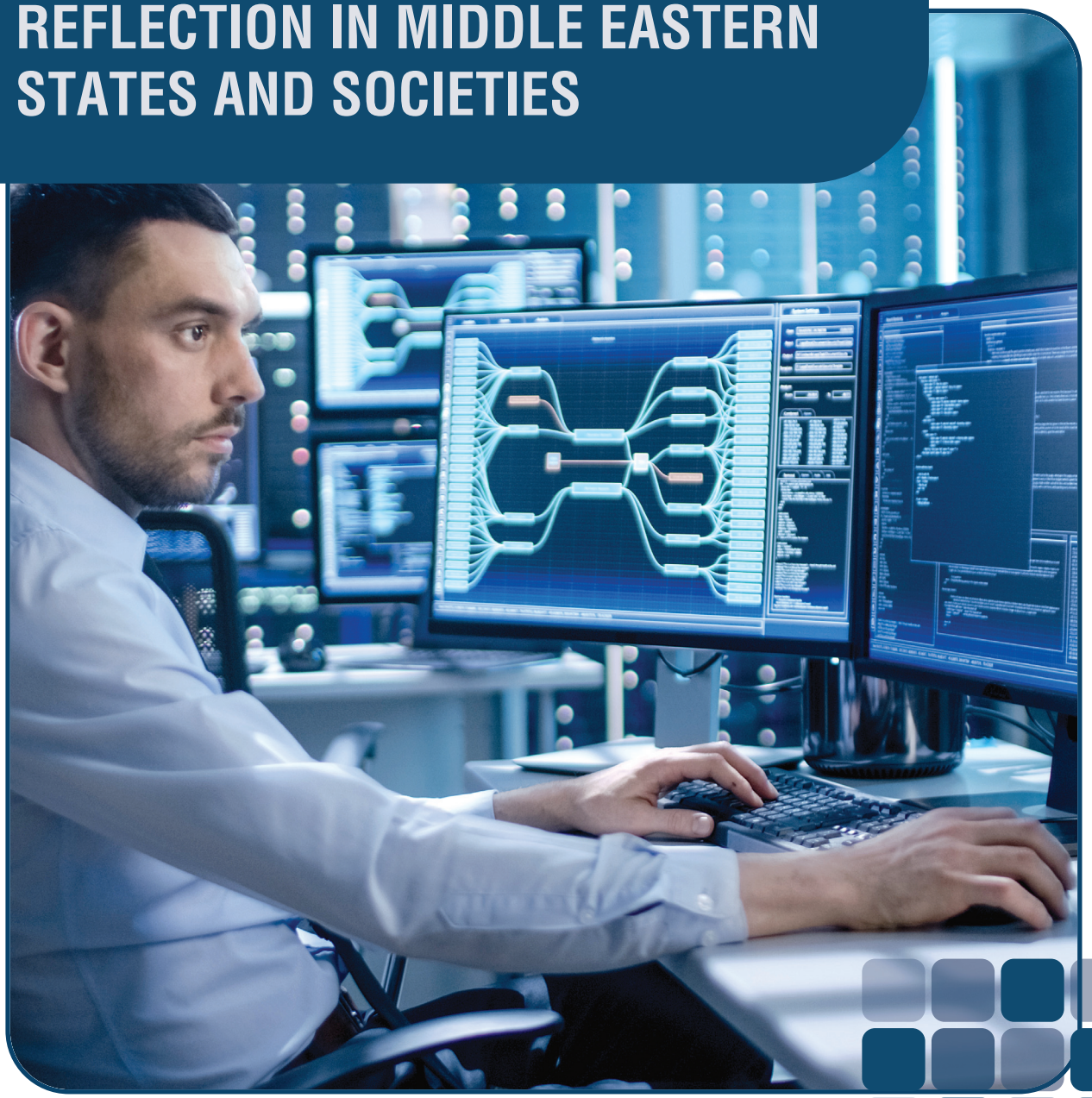
Ortadoğu Araştırmaları Merkezi
ORSAM
مركز دراسات الشرق الأوسط
Center for Middle Eastern Studies

Report

No: 23 / December 2020

CONTROVERSIAL ISSUES IN GLOBAL INTERNET GOVERNANCE AND THEIR REFLECTION IN MIDDLE EASTERN STATES AND SOCIETIES



H. KÜRŞAD ASLAN, İKRA ERCANLI

Copyright

ISBN: 978-625-7219-13-6

Center for Middle Eastern Studies

Adress : Mustafa Kemal Mah. 2128 Sk. No: 3 Çankaya, ANKARA
Phone : +90 850 888 15 20
Email : orsam@orsam.org.tr
Photos : Anadolu Agency (AA), Shutterstock

According to the second paragraph of Article 5 of the Regulation on Banderole Application Procedures and Principles, the use of banderole for this publication is not compulsory.

Ortadoğu Araştırmaları Merkezi
ORSAM مركز دراسات الشرق الأوسط
Center for Middle Eastern Studies

REPORT

CONTROVERSIAL ISSUES IN GLOBAL INTERNET GOVERNANCE AND THEIR REFLECTION IN MIDDLE EASTERN STATES AND SOCIETIES

About the Authors

Assoc. Prof. H. Kürşad Aslan

In 1994, Dr. Aslan received his undergraduate degree from the Department of Political Science, at the Middle East Technical University in Ankara. In 1999, he completed his MA thesis titled "Azerbaijan's Oil in Regional and Global Politics" and graduated from the International Relations and Political History program in the Institute of Middle East and Islamic Countries at Marmara University. In 2011, Mr. Aslan obtained his Ph.D. degree from the Department of Political Science at Kent State University in Ohio with his dissertation titled "International Labor Migration from Rural Central Asia: the Potential for Development in Kyrgyzstan and Uzbekistan." Between 2011 and 2015, he worked as an assistant professor at Eskişehir Osmangazi University. He has also been working at Istanbul Medipol University, in the Department of Political Science and International Relations since 2015. Associate Professor Aslan's main research areas include global political economy, foreign aid, foreign policy, research methods, and Eurasian politics.

İkra Ercanlı

İkra Ercanlı was born in 1998 in İstanbul and she is now pursuing her BA degree from the department of Political Science and International Relations at İstanbul Medipol University. İkra has gained a variety of practical experiences from research projects with her professors, the TÜBİTAK Migration Project with Assoc. Prof. H. Deniz Genç, and Health Tourism Project with Assoc. Prof. H. Kürşad Aslan and H. Deniz Genç. She has also worked with the Foreign Economic Relations Board of Turkey (DEiK) as an intern.

December 2020

CONTENTS

TABLE

1. INTRODUCTION

Governance of global commons, including global internet governance, is becoming more and more complex as the world's political order has been in flux especially in the past two decades. These controversial issues have frequently become intertwined between national regulations and international law. As one of the most important global public goods, cyberspace is highly competitive and nation-states confront each other due to their conflicting norms, values, rules, and principles regarding internet governance. Sometimes like-minded states work together and attempt to enforce their own rules and regulations and resist the existing internet governance regime around the globe. Joseph Nye (2014) maintains that the internet is ad hoc regulated through a newly emerging cyber regime complex, and this regime has dense regulation in some subject areas but is largely unregulated in some other issue areas.[1]

In the first part of this report, main actors and two rival blocs in the global cyberspace governance, principles of the internet design, and competing norms of the Western (USA and EU) and Eastern camp (China and Russia) will be discussed. In this complex political environment, middle powers of the Middle East (predominantly Iran, Saudi Arabia, and Egypt) along with some others are taken as cases with their diverging positions. And it is interesting to observe that these Middle Eastern nations have been following dualistic policies in their external and internal political context. Therefore, in the second part, national policies of these governments about internet governance will be analyzed. It can be seen that as the global political order has been shifting towards being more of a multipolar type, middle powers tend to follow hybrid national policies. As critical international relations theoretician Robert Cox suggests, the middle-power role continually evolves.[2] In the past two decades, we can observe the appearance of a group of emerging middle powers in the global political economy; and Goldman Sachs has conceptualised a list of eleven countries, titled the "Next 11" and within this group worth mentioning are Egypt, Indonesia, Iran, Nigeria, Pakistan, and Turkey.[3] Therefore, capturing and identifying the nuances of the foreign policy behavior of the emerging middle powers of the Middle East will be recorded as being a very valuable academic effort. This report presents a case study to highlight the policy choices of middle powers in the Middle East region in the face of fluctuating global politics.

2. GLOBAL GOVERNANCE OF THE INTERNET

For more than half a century, computers have been noticeable in public life. And for the last two decades, the use of the internet has accompanied us in the routines of our daily, social, economic and political life. These two technological factors play important roles in the global communications and informatics world and are increasingly becoming intertwined with the lives of people around the world. Therefore, this field of activity can be envisioned as a social field or a large area that needs to be regulated by the nation states or perhaps a well working international regime.

Initially, in 1969, the US Department of Defense designed a system called ARPANET (Advanced Research Projects Agency Network), which consisted of several computer connections, and the World Wide Web as we use it today came to life in 1989. Cyberspace has been recognized as a new arena for competition among national governments not only for

security reasons but also for economic returns. In the global digital economy framework, there is an effective combination of hardware and software, time and data, surveillance, forecasting and behavioral control. According to Chinese sources, the size of Beijing's digital economy reached approximately four trillion US dollars as of 2017, contributing 55 percent of the growth in national income. In the same year, China and the USA were the top contributors to the global digital economy with a size of approximately 13 trillion dollars.[4]

There were only a million users on the internet in the early 1990s; and now the number of users has increased from 1.9 billion in 2010 to 4 billion by 2020.[5] It is projected that the internet access of the global population will increase from 47% in 2017 to 54% by the end of 2021. In 2021, it is expected that the proportion of smartphones with internet access that we all use will reach to 1 in 4 among all networked devices. The global cybersecurity market is currently worth $173 billion in 2020, and it is estimated that it will reach to $270 billion by 2026.[6] Many states are restructuring their security organizations and institutionalization processes: cyber space has started to be defined as the fifth domain of warfare after land, sea, air and space.[7]

Many controversial issues in the field of global internet governance are becoming more and more complex. It is an undisputable fact that the world's political order has been in flux, and many academics and policymakers do not know what is necessary to build the new world order and when it will happen. As it is the case for many global public goods, internet governance is also emerging as one of the problematic issues of twenty-first-century global governance. In the last few decades, the pace of technological developments has been rather fast; and global and regional institutions have been insufficient to build legal and political infrastructure in response to these changes and transformations.[8] There is no doubt that global and regional actors need to find new solutions and responses due to recent paradigms like the real-time control system, the transfer of voice, text or video and future applications.[9]

The controversial areas that have been observed in the governance of global public goods are often due to the excessive emphasis on state sovereignty, the inflexibility of national regulations and the inefficiencies in the production of international law. Problems and debates that remain unresolved in internet governance require coordination and alignment in many different legal and political sub-areas, including the United Nations Charter, armed conflict laws, the availability of infrastructure, international trade, security, intellectual property laws, and freedom of expression and privacy among others.

It would be helpful to remember a few examples from certain flash news events such as the publication of secret information by Julian Assange's WikiLeaks, the Russian government's alleged interference in the 2016 U.S. presidential elections, the disclosure of the Stuxnet computer worm, the state induced Egyptian internet outage, increasingly frequent and sophisticated cyberattacks, North Korea's hack of Sony Pictures, global tension over the United Nations international treaty conference known as the International Telecommunications Regulations (ITRs), disclosures about the National Security Agency's (NSA) expansive surveillance programs, and the release of the Mandiant report, which disclosed the existence of Chinese units cyber-spying on the United States.[10]

On October 4, 2018, the United Kingdom made an official announcement that strongly denounced "reckless" and "irresponsible" cyberattacks conducted by the Russian military intelligence service against a wide range of targets, including the Organization for the Prevention of Chemical Weapons, the United Kingdom's Foreign and Commonwealth Office, and its Defence and Science Technology Laboratory. In the official note it was highlighted that "The UK Government judges that the Russian Government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack of June 2017. The attack showed a continued disregard for Ukrainian sovereignty. Its reckless release disrupted organisations across Europe costing hundreds of millions of pounds." The UK statement emphasized that these attacks were violation of international law and established norms.[11] WannaCry and NotPetya cyber attack operations with strong indications of originating from North Korea and Russia show the extent of the vulnerability in the digital space; economic damage of NotPetya is estimated at roughly $ 10 billion.[12]

In relation to these caveats, the internet has serious new security challenges for national governments. New threats have emerged such as cyber-warfare, cybercrime, cyber-terrorism, cyber-espionage and the like.

In the literature about global governance of the internet and the national security dimension of cyberspace two issues have been highlighted.[13] First is that the fundamental problem structure underlying internet governance has changed from a purely technical coordination game towards a problem of cooperation.[14] The second is about the political economy of information technologies including the internet.[15] It seems that distributional conflicts are becoming more compound and severe. Thus, this is a new hybrid problem structure. Distributional impacts spread within both the domestic borders and interstate affairs. Thus, the contentions have associated with the distribution of material benefits among nations. In other words, the coordination of the internet and its governance is above and beyond the mere technical administration issue at the global scale.

In relation to these caveats, the internet has serious new security challenges for national governments. New threats have emerged such as cyber-warfare, cybercrime, cyber-terrorism, cyber-espionage and the like. According to institutional theory, a well functioning institutional framework provides an incentive structure, diminishing transactions costs and reducing uncertainty. These institutions shape main actors' behaviors.[16] Regarding the governance of the World Wide Web main actors do not feel that there is a reliable incentive structure.

There is no change in national governments' distrust of each other. Cyberspace can be considered to be a very good example of the cyber security dilemma in such an environment of insecurity. It should not be hard to understand the possibility that misunderstanding and misinterpretation in cybersecurity can turn into a dangerous security spiral.[17] All of these problems make internet management a very problematic issue area. The race to penetrate this world of computing between states creates a "security dilemma" in which

no state can understand the intention of the other in cyberspace.[18] The skepticism and lack of trust among the major actors push each side to take protective countermeasures, which ultimately creates a vicious cycle. Beijing has been accused of a systematic state-led cyber campaign against the US, Britain and their Western allies aimed at stealing secret information from governments and high-tech companies in one of the most wide-ranging cases of corporate espionage on record. Thus, information security constitutes a point of contention in the U.S.-China relationship.

The Trump-led US administration ranks espionage, cyberattacks and intellectual property theft at the top of its accusations against Beijing and its demands for change. In August 2020, President Trump demanded from the Chinese tech company ByteDance that they sell TikTok to an American firm due to the potential security threat to American interests. TikTok, the popular short-video application, has more than 100 millon users; and Washington DC explained that users' data is open to manipulation by social engineers and is likely to be sent to the company's headquarters in China.

On the other hand, new IP is expected to support new applications with expected high market shares like telemedicine and holographic communications. Thus, Western governments are deeply concerned over Chinese technological advancements, particularly those being developed by Huawei. These are, more specifically, the advancements of 5G, which promises an automated world, and electronic products developed by Huawei. Despite all these concerns about espionage, the fact that Chinese companies have invested the most in internet infrastructure worldwide in recent years undermines the credibility of Western statements. While Beijing signed agreements with many countries within the framework of the "Digital Silk Road" concept, on the other hand, Huawei has a contract with approximately half of the countries registered with the UN for the construction of a 5G wireless telecom infrastructure.[19]

Attempting to control cyberspace, nation-states are influenced by both domestic and global dynamics. For many states, the internet is also important in the context of internal stability and security. During elections and public demonstrations governments are willing to employ several regulatory methods to halt politically disruptive actions within their territories. The recent colorful revolutions and Arab Spring movements have taught the emerging powers critical lessons. For instance, after the uprisings in the Arab world, Russia started to closely monitor the impact of the political use of a networked technology upon social mobilization and democratic transition.[20]

> At one end of the poles is the Western World, led by the USA. On the other hand, we see the Eastern camp, mainly led by Russia and China, who argue that current international law does not cover cyberspace. The Eastern camp, following a revisionist attitude, defends the thesis that new conventions are needed as a prelude for a new regime regarding internet governance.

National governments with similar national security cultures and strategic interests have

been coming together more and more in recent years and are influenced by each other's policy practices. The competitive cyberspace environment naturally brings about a tension between older norms, rules, and principles and those that are gradually displacing them.[21] Nocetti (2015) defines internet governance as "all shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the internet" which had been proposed earlier by the UN-initiated first World Summit on the Information Society (WSIS) in 2005. In the following section we focus on the rival blocs, competing norms and major actors along with aborted institutionalization processes.

3. RIVAL BLOCS, COMPETING NORMS AND INSTITUTIONS

3.1. Rival Blocs

Two big blocs have emerged in the debate about the future of global internet governance and related norms. This polarization stems from differences in ideological and strategic interests between the great powers.[22] At one end of the poles is the Western World, led by the USA. On the other hand, we see the Eastern camp, mainly led by Russia and China, who argue that current international law does not cover cyberspace. The Eastern camp, following a revisionist attitude, defends the thesis that new conventions are needed as a prelude for a new regime regarding internet governance.

According to the thesis of the Chinese and Russian wing, global governance should adopt state-centered decision mechanisms: there is a demand for change from the multi-stakeholder approach towards a state-led global cyber-governance regime. We observe the diverging preferences of individual states with regard to the internet's basic principles. The critical issue of debate about internet governance revolves around a more liberal or more government-oriented global governance decision model.[23]

China's general position on global cyberspace governance is based on the "multi-stakeholder, democratic and transparent" model. However, what Beijing conceptualizes in these terms is different from Western countries. The most critical concept is the multi-stakeholder management. China's position is that the construction of a global internet governance system requires multilateral participation only by sovereign states. While Western countries generally interpret "multilateral" to mean the support and participation of all private and/or public institutions as stakeholders; China places more emphasis on the equal participation of all nation states in global policymaking.[24]

There are many similarities between the positions of Moscow and Beijing on global internet governance. Moscow prioritizes its domestic stability due to the fear that the "colored revolutions" and mass uprisings might well be duplicated in Russia where there is a large volume of non-Slav and/or non-Christian minorities.[25] For China the same logic applies. The Chinese Communist Party has given top priority to stability and security and recent Hong Kong protests and concerns of territorial integrity due to secessionist claims of the Uighurs and the Tibetans for decades caused Beijing to increase all sorts of authoritarian security measures. Authoritarian regimes, including Russia, Saudi Arabia, Iran, Egypt, and China, seek to monopolize internet infrastructure, filtering web content or slowing internet speed when civilian tensions are high. These regimes have learned that the internet must be shut down to impair the ability of protesters to coordinate and broadcast in real time resulting in tensions threatening the survival of the regime in the country.[26]

On the other hand, we have seen during the "colored revolutions," the Arab Spring mass movements and the Green Movement in Iran that the internet provided ordinary people with opportunities and turned them into "voluntary journalists," breaking the government's monopoly over producing and broadcasting news.[27] In sum, authoritarian regimes favor a very interventionist approach to internet control. For example, the Communist Party of China does not want an ordinary Chinese citizen to be confused with Western internet resources, and a virtual "Great Firewall" was built to prevent this.[28]

Many governments have been increasingly allergic to US hegemony over the internet; therefore, these countries are trying to challenge the role and dominance of the United States in cyberspace.[29] Russia and China are trying to end the USA's dominant position through regional forums. The concepts of "digital colonialism" and a "military-digital complex," which are frequently used in critical approaches, reveal the root causes of disturbances; critical arrows of this kind now come not only from the underdeveloped authoritarian states, but also from Europeans.[30] According to experts, in an environment of deep competition regarding global internet governance, the European Union prefers to be positioned

somewhere in the middle of the two rival camps.[31]

Russian President Vladimir Putin once said the internet was developed by the US as a "special project" by the Central Intelligence Agency and warned Russians against making Google searches. Putin told journalists that Google's web traffic "goes through servers that are in the United States," and "everything is monitored there."[32] At the root of the dominant role of the United States in the internet governance regime is its control over the Internet Corporation for Assigned Names and Numbers (ICANN). This authority is based on a contract between the organization in question and the US Department of Commerce.[33]

Therefore, the Russian Duma initiated a new law that obliges social media websites to keep their servers in Russia and save all information about their users for six months.[34] This is due to the fact that, of the 13 root servers of the entire internet, ten are located in the United States, and the other three are on the territory of US allies: Japan, the Netherlands and Sweden. As of September 2020, among those root servers one is located in NASA (Ames Research Center), another is in the US Department of Defense, and the third is in the USA Army's Research Lab.[35] Basic information about 13 root servers and their operators can be seen in the table below.

Root servers are something like train stations. The Domain Name System (DNS) con-

Table 1: List of Root Servers in the World

#	Host Name	Operator
1st	a.root-servers.net	Verisign, Inc.
2nd	b.root-servers.net	University of Southern California, Information Sciences Institute
3rd	c.root-servers.net	Cogent Communications
4th	d.root-servers.net	University of Maryland
5th	e.root-servers.net	NASA (Ames Research Center)
6th	f.root-servers.net	Internet Systems Consortium, Inc.
7th	g.root-servers.net	US Department of Defense (NIC)
8th	h.root-servers.net	US Army (Research Lab)
9th	i.root-servers.net	Netnod
10th	j.root-servers.net	Verisign, Inc.
11th	k.root-servers.net	RIPE NCC
12th	l.root-servers.net	ICANN
13th	m.root-servers.net	WIDE Project

Source: IANA, 2020.

verts internet domain names into numeric addresses. The authoritative name servers function something like decisionmakers so as to find top level Domains (like .tr for Turkey addresses). From the generic top-level domains (such as .com, .net, and .org) or country code top level domains – two-letter codes for each country, (such as .tr for Turkey or .ru for Russia) we understand the sources of the internet's components. For example, when we see the web site address of the ORSAM (https://orsam.org.tr/) we make deductions that it is an organization in Turkey. The root servers are operated by 12 different organizations and 13 numeric IP addresses that could be seen in the Table. Verisign operates two root servers, and all others operate one. Each operating organization is solely responsible for the root server IP address it operates.

Russia prioritizes UN-led international organizations and regional forums to spread Moscow's top down approach to internet governance.[36] In 1998, Russia submitted a resolution to the UN's First Committee on "Information and Telecommunications." Russia has been making proposals to the United Nations for new global regulations every year since 1998. According to this approach, attempts at "information aggression" over the internet by ideological or other propaganda-oriented initiatives should be prevented from undermining the stability of regimes. Russia maintains that the International Telecommunication Union (ITU) should be at the center of the internet governance at the globe. The International Telecommunication Union (ITU), which was founded in 1865 to facilitate international connectivity in communications networks, is the United Nations' specialized agency for information and communication technologies.

Moscow also argues that the internet is an essential component of the global telecommunications infrastructure and therefore should be negotiated in appropriate global internet governance processes. Many other States, including Iran, Sudan and Bahrain, are of the same view with Russia and the idea to revise ITRs to include internet governance issues. In November 2018 a cybercrime resolution by Russia was adopted by the UN General Assembly and the three biggest democracies in the world—India, Brazil, and Nigeria—voted with Russia and China.[37] It is worth remembering that Russian speaking countries as well as China and India had put forward a proposal to give governments oversight power (via the ITU) above the decisions of the ICANN on naming and addressing in 2010.[38] Essentially, governments who share the same strategic interest attempt to de-Americanize the internet.

In the field of internet governance, it is important to highlight the position of the European Union and its major actors (Germany and France), its deviations from the USA and its similarities with the Eastern camp. In 2004, the European Union Agency for Network and Information Security (ENISA) was established regarding the governance strategies of European cybersecurity, and each year its power and responsibilities have increased. The EU faced a fast-paced threat landscape in world politics and a stalemate with the international cyberspace convention, as well as debates about global norms and responsible state behavior. The fact that the European Union has different attitudes from both the Americans and the Eastern camp to a large extent reveals an interesting picture in finding the global balance. In June 2017 the European Union made a new initiative; the decision was made

to develop a comprehensive framework for a common EU stance on cyber attacks and a bundle of countermeasures called the Cyber Diplomacy Toolbox.[39] The President of the European Commission Jean Claude Juncker presented the digitalization of the European economy and society as one of the most pressing issues in his 2017 State of the Union speech. On 13 September 2017, the Commission adopted a new cybersecurity package, within which the Cybersecurity Act remains at the core of the package. The cyber package touched many aspects of the European governance, regarding the digital economy, but increased tremendously the role of the ENISA.

3.2. Competing Norms

Looking at the political science literature, we can see that global norms can emerge and spread in many different ways. In the discipline of International Relations, the dynamics of the development of norms and the process of general acceptance among the global society have been investigated in a way that is verified by detailed and empirical data. Finnemore and Sikkink (1998) proposed the norm life-cycle model; and another alternative model has been presented by European political scientists in the form of the "spiral model."[40] At the national level, norms can arise in different ways, for example from habits or decentralized national legislation by norm entrepreneurs or from practices. Its origins can be either national governments or international actors. The emergence of the norm can come from the bottom up, leading to institutionalization of what kind of behaviors are appropriate in particular situations for actors who have a certain identity in their cultural context. Alternatively, the emergence and propagation of the norm can come from top to bottom; in this case, institutionalization processes will work with different mechanisms.

Since internet governance is a very new field, giant technology companies in the information and telecommunication sector can also play a role in the formation of the norm structure in this regard. As the main motivation of these private sector actors is to make a profit, an interesting process can be observed with the private-public sector interactions in the birth and evolution of norms. The role of private actors could be best explained within the framework of the liberal theoretical tradition. The liberal perspective maintains that the internet is a collective (or public) good.[41] Therefore, the liberal perspective sees the development of internet norms as a collective problem. For this, the liberal view argues that the internet can enter the process of institutionalization by its stakeholders, private and public sectors (including companies and states) could work together.

In recent years, cybersecurity tools are becoming a huge market. This exponential increase in this new security market is a result of a growing cyber arms race. Some companies offer services and tools for offensive cyber-attack operations. The market for internet filtering and censorship, as well as for offensive cyber-attack operations and surveillance has also exploded in recent years in response to governments' attempts. For example, many authoritarian countries have used US-based commercial filtering products including Fortinet in Burma, Websense in Yemen and Smartfilter in Iran and Tunisia throughout the 2000s.[42]

In the governance literature scholars analyze a number of initiatives started by private actors that aim to influence the global debate

about cyberspace governance. Microsoft is very active in the international debates about global cyber-norms.[43] Microsoft and Siemens are two prominent actors within the Global Commission on the Stability of Cyberspace (GCSC): this institution recently published a report about state and market interactions.[44] The GCSC was born at the 2017 Munich Security Conference; and its mission is specified as building new policies and norms so as to improve global security and stability along with prescribing responsible state and non-state behavior in cyberspace. Another initiative was launched by the French government named the "Paris Call for Trust and Security in Cyberspace" and it began in November 2018 with the sponsorship of the recently founded Cyber Peace Institute.

Another major private initiative that should be mentioned is the Global Internet Forum to Counter Terrorism (GIFCT); this independent (industry-funded) initiative was established by Facebook, Microsoft, Twitter, and YouTube in 2017 to prevent terrorists and violent extremists from exploiting digital platforms. This forum was designed to foster technical collaboration among member companies, advance relevant research, and share knowledge. It is also worth mentioning the Global Extremism and Technology Network (GNET) as a research initiative launched by the Global Internet Counterterrorism Forum (GIFCT); GNET was brought together by the International Centre for the Study of Radicalization (ICSR), a globally renowned academic research center in London.

Principles concerning the internet, whether technical or normative, have had both social and technological significance. While some normative principles regard the internet as a global common and determine the internet's standard, some others are related to engineering principles which are designed to make the internet function more efficiently.[45]

The end-to-end (e2e) is one of the foundational principles of the internet design that organizes the placement of tasks within a network. The e2e arguments have two complementary goals: first, application autonomy and second, network transparency.[46] Although it was initially adopted for purely technical reasons, the principle of e2e has evolved towards a feature beyond its technical aspect, including normative values and ideological approaches. By enabling many applications to use and connect to the network, it creates competitiveness and increases the number of units competing for network usage. It provides everyone an ability to implement a better way to use the internet connection without discrimination in the use of network. Moreover, in the early years of e2e, the guiding principle of internet design, there was a commitment to exemption from government intervention in the context of accessing applications and services and that users would not be discriminated against.[47] All data should be equally available to all internet users without any intervening and discriminative principles about the speed, price and access of the information.[48] In addition, the use of applications on the network and the development and distribution of new ones can occur in an environment of complete freedom.

Another very important basic principle associated with e2e is network neutrality which can be defined as the "right of users to access content, services and applications on the internet without interference from network operators or government," and the "right of network operators to be reasonably free of liability for transmitting content and applications deemed illegal or undesirable by third parties."[49] In other words, this norm entails a non-governmental type of internet governance.

The internet and other communication tools initially emerged as a global common in a highly liberal and non-interventionist environment. The e2e and other associated principles of net neutrality have changed in time. With the changing threat perceptions of states and new control practices discovered in political processes over time, what is called "norm regression" in global internet governance has been occurring.[50] State control, which is an increasing trend in the world of information and communication, has triggered the process of change in the normative structure of cyberspace, which is defined as completely free and open.

Governments have put in place different control mechanisms such as information control; they started to see actions to change, control or manipulate content on the internet as a necessity in light of some criteria such as national security or public health. At the international level it is very difficult, in practice, to establish a global consensus on common issues pertaining to moral, religious and public order values even in regard to child pornography or human trafficking. However, at the national level public opinion may press governments to intervene with some crucial issues.

For instance, China imposed restrictions on accessing the internet in Xinjiang for 10 months as a result of the ethnic riots and it also blocked Twitter because the violence was first reported by videos and photos, The Chinese government brought media regulations and content removal and filtering on the incident. Censorship or internet filtering which means to block the access to information within territorial boundaries is another form of government control. The report by the OpenNet Initiative, which deals with national

internet filtering, has shown that more than 40 countries engaged in censorships regardless of whether they are democratic or authoritarian regimes. While a great number of them are democratic countries, non-democratic ones engaged in internet filtering by using these tools developed in Western democratic countries such as the United States and Canada.[51]

Another side of the state-society relations and the social contract is related to the human rights dimension. In many countries, citizens cannot fully enjoy their fundamental freedoms, which they should exercise, such as their freedom of expression and their rights as a natural consequence of human rights. This is because they are afraid of the excessive control mechanisms of governments. On the contrary, internet and information technologies may provide governments with some technical means to monitor citizens and control their fundamental rights. In other words, the internet may be used as a tool of repression in authoritarian states. For instance, citizens are better surveilled thanks to artificial intelligence and massive databases of information about them are collected.[52]

Chinese tech companies including giant Huawei assisted the Russians to increase their capacity to monitor and built their own web system.[53] In Russia, the "sovereign internet law" passed, and it entered into force on 1 November 2019. This new legislation allows the Russian government to practically separate the internet from the rest of the world. It also allows Moscow to further tighten the country's control and surveillance of the internet by routing its web traffic through state-controlled infrastructure and creating a national system of domain names. Theoretically, the measure could allow Russia to detach from the rest of the World Wide Web and operate its own local internal networks that can operate independently.

We observe that internet norms are spreading in various platforms where countries with similar ideological and mental structures come together. Governments have been steadily becoming influential actors and they promote their corresponding norms and practices. The most important systemic and global forums in internet governance are the Internet Corporation for Assigned Names and Numbers (ICANN), the International Telecommunication Union (ITU), and the Internet Governance Forum (IGF). Russia has been very actively engaged in reform of these international institutions and their working principles. Russian President Vladimir Putin argues that the United Nations should be at the center of the global cyberspace regime and that the ITU is the most appropriate institution in terms of legitimacy and technical capacity for internet regulation.[54]

The differing views on internet governance reflect the general attitudes and perceptions of national governments regarding democratic rights and civil liberties as well as their internal political culture.[55] As a result, the focus of these institutions has shifted from technical issues to politicized ones. For example, Russia and China emphasize state sovereignty as a primary principle in terms of internet management, and they see internet control as a natural result of sovereignty. Therefore, these countries have made it clear that cyberspace should be managed by global institutions operating within the UN.[56] Cyber-sovereignty is frequently stressed by Russia and China.

Claims of sovereignty have justified reasons in recent history. For instance, "colored revolutions" and the Arab Spring have been alarm

bells for many countries. Those cases, and some other domestic upheavals have become the pressing factors for many states to expand their capabilities for monitoring and disrupting online communication during mass protests. Additionally, these governments also learned to use digital technologies to shape public opinion, mobilize supporters, and track emerging grievances.[57] Thus, many governments and their security agencies started to closely monitor the networked technologies, social media applications and their mobilization potentials.

Western countries, especially the USA and EU members, emphasize the multi-stakeholder approach to governance. A multi-stakeholder model in cyber governance brings governments together with civil society, non-governmental organizations, businesses and, research institutions in the process of implementation, cooperation, and decision-making. The United States and others suggest free and open information without the interference of governments on the internet. ICANN, a primary global institution on internet governance, is an example of a multi-stakeholder organization in which the influence of governments declines in the decision-making process due to the involvement of non-governmental organizations and private sectors.[58]

"Cyber sovereignty" should be noted in terms of defining the breaking point in the Western and Eastern world. Cyber sovereignty is the core principle that China promotes in global cyber governance. The Chinese approach to global internet governance can be labeled as multilateral pluralism based on cyber sovereignty.[59] Cyber sovereignty is based on the political-cultural thoughts, norms, values and interests of a state's sovereignty and its ability to protect its infrastructure active on the internet.

As a result, we can note and highlight two main trends regarding cybersecurity and internet governance here. First, a definition of national sovereignty in cyberspace should be made, just like in physical zones. The second important trend is that rapid technological changes unfortunately caused the legal infrastructure to lag behind. In other words, there is no moral, ethical, and legal collective understanding and consensus on the global governance of the internet such that the entire international community can come together with a common understanding.[60]

3.3. Global Institutions and Failed Institutionalization

In the face of the increasing pace of technological advancements and evolving geopolitical conditions we observe an increasing tone of securitization in the cyberspace realm. The Washington administration first issued the 2011 US 'international strategy for cyberspace'. Later in the official American documents the frequency and importance of cyber threats have gradually increased. The term "cyber" numbers 46 times in the USA's December 2017 National Security Strategy. The 2017 National Security Strategy has labeled China (and Russia) as the "strategic competitors" and the "revisionist powers," and those countries put the American national interest at risk by exploiting vulnerabilities across the land, air, maritime, space, and cyberspace domains. On the other hand, Russian officials prefer to use the "information space," rather than using the term "cyberspace" and it is noteworthy that Moscow has not publicly released any national strategy documents which specifically focus on cyberspace.[61] The most

relevant cyberspace strategy document could be the Information Security Doctrine of Russia. The most recent version of this document is dated December 2016.[62]

In the field of internet governance, ICANN is the institution at the focal point of global governance. A private and multi-stakeholder organisation founded in 1998 in the United States, ICANN has authority over the internet through its power to manage internet protocol addresses and the domain name system.

The first and most important conferences that were convened to discuss demands for innovations in global internet governance were held since the early 2000s. In 2003, the United Nations General Assembly adopted a crucial resolution, the "Creation of a global culture of cybersecurity" during the 57th Annual Session. The UN General Assembly, which was held on 21 December 2001, endorsed the holding of the World Summit on the Information Society (WSIS) in two phases. The first phase took place in Geneva in December 2003 and the second phase took place in Tunis, in November 2005. The main objective of these conferences was to develop and promote a clear declaration of political discretion and implementing necessary steps to establish the foundations for a global information society for all people, taking into consideration the interests and opinions of all stakeholders. The Geneva Phase of WSIS brought about the final declaration with the name, the "Geneva Declaration of Principles" and the "Geneva Plan of Action." The Second WSIS Summit had a variety of public and private sector representatives from 174 countries as well as high-level representatives from international organizations. The output was the "Tunis Commitment and Tunis Agenda for the Information Society."

Another prominent institution is the ITU, the International Telecommunication Union, which has become the effective standards body for telecom networks. For some governments, those standards decided by the ITU legitimize new technologies and systems. China, Russia, Iran, Brazil and other emerging powers give importance to domestic defense systems and other high-tech systems including communication and information infrastructure based on the same nationalistic logic. At the policy level, all the BRICS states have put great emphasis over internet management and cyber security. Despite the increased institutionalization of the BRICS as a coalition and despite various proposals contesting the role of the Western world, primarily the United States, regarding the internet we see that BRICS countries have not been able to set a common policy framework in a coherent, systematic and single voice.[63]

In the field of internet governance, ICANN is the institution at the focal point of global governance. A private and multi-stakeholder organisation founded in 1998 in the United States, ICANN has authority over the internet through its power to manage internet protocol addresses and the domain name system. The role of ICANN as a policy making body has been challenged in time with political implications. ICANN allocates "country code Top Level Domains" (ccTLD) (.uk, .au). IP addresses have run out under the protocol of IPV4. Although China has more than half a billion in-

ternet users, 74% of IP addresses have been allocated to the US. According to Carr (2015), the ccTLDs legitimize a sovereign space and characterize national cyberspace. Considering ICANN as an effective mechanism and authority, this disparity in the distribution of IP addresses indicates the Westphalian global internet governance, creating a concern for emerging powers.[64]

Another example is that a US Court decided on hundreds of millions of dollars in compensation from Iran resulting from a Hamas suicide bombing in Jerusalem. When the plaintiffs asked ICANN to seize Iran's ccTLDs and submit these to the plaintiffs, ICANN opposed their demands for political, legal and technical reasons. However, this led the question of whether ccTLDs should be controlled by a private organization, a non-profit company or an international agreement.[65]

Nation states often view the particular institutional set up of ICANN as problematic for two reasons. First, ICANN is based on a multi-stakeholder model where the private sector and non-governmental organisations play a major role, decreasing the influence of states to shape the policies and practices of this organisation. Second, oversight authority of the US Department of Commerce over ICANN and the physical presence of ICANN inside US jurisdiction, creates the appearance of undue US influence over the organization.[66]

Another institutionalization initiative is the UN Group of Governmental Experts process, which was started in 2004, to create a high-level discussion forum at the UN level. As of 2017, GGEs (Groups of Governmental Experts on Information Security) had three major discussions on basic norms and confidence-building measures for cyberspace, starting from 2010.[67] The 2017 session was aimed at harmonizing cyber technology and international law. Five rounds were completed by 2017, and the group of experts prepared three plenary consensus reports (UN General Assembly 2010, 2013, 2015). After the 2017 round, the UN GGE had come to a breaking point due to the failure to reach a common consensus.

There were ideological reasons behind the UN GGE's failure to agree on a consensus report in 2017. The Eastern and Western camps had insisted on their own normative structure. The main view of the Western camp presupposed the application and interpretation of existing international law with minor changes. The Russia-China camp focused on more radical reforms, with the establishment of a new regime. While the Eastern camp promoted state sovereignty and tight control of the internet, the Western camp prioritized a multi-stakeholder internet governance approach based more on individual freedoms and human rights, as well as the openness of cyberspace.[68]

After the 2017 deadlock on the UN GGE series, surprisingly, in November 2018 the UN General Assembly voted two parallel and competing bills. In the first motion, the USA called for a new round of the GGE. The second motion was proposed by Russia and called for the Open-Ended Working Group (OEWG) to negotiate issues similar to the American proposal. Both entered into force as a result of the deliberation at the UN General Assembly from November 2019 and the twin negotiation process resumed.[69]

Another example for institutionalization of cyber governance is NATO's publication of the Tallinn Manual, which sets out to define the legal framework applying to cyberwarfare.

According to scholars, "The Tallinn manuals are the most comprehensive analyses of International Humanitarian Law and cyberspace available and serve as an important reference point."[70] The "Tallinn Manual 2.0 was published in 2017, updating the 2013 analysis on how existing international law applies to cyberspace.[71] The Tallinn Manual and the UN GGEs are highly important documents that came into being over a long period of time and bring together internationally acceptable good practices.[72]

Another major example of the ideological divide in the institutionalization processes of global internet governance is the Budapest Convention and the International Code of Conduct on Information Security. The Budapest Convention is the first international treaty that aims to increase cooperation between governments on cybercrime. The convention also represents the division between Western and Eastern views on the use of information and communications technology. All member states of the Council of Europe as well as the United States have ratified the Convention. On the contrary, neither China nor the members or observer state of the Shanghai Cooperation Organization has ratified it due to their perception of the convention as violating the sovereign right of a state.[73] Besides, The International Code of Conduct on Information which was submitted to the UN General Assembly in 2011 is another example showing the ideological differences. The code is an international effort to develop norms of behavior in cyberspace.[74] In 2015 the code was revised by the members of the Shanghai Cooperation Organization. It emphasizes the sovereign right of states to regulate the use of information and communication technologies.[75] Therefore, both international efforts and regional initiatives represent divergent approaches of nation-states in the use of ICTS.[76]

The ideological polarization manifested itself in another environment in 2012. Member states had been divided over the new International Telecommunication Regulations at their meeting. The separation followed the lines indicated. On the one hand, the United States and several European Union states supported the liberal approach and light regulation. On the other hand, Russia-led states supported government participation and stricter regulation. For example, a coalition of Russian-speaking countries, supported by China and India, have put forward a proposal to give governments veto power over ICANN decisions.[77] Only 89 ITU member states signed the final act of the 2012 World Conference on International Telecommunications. The USA and several European states were not among the signatories of the final act.[78]

The World Conference on International Telecommunication, or WCIT, held in December 2012 was an important milestone. The WCIT – 2012 summit came together in Dubai between December 3-14. The existence of a wide spectrum of approaches emerging in the field of internet governance has attracted considerable attention. Many governments have challenged the multi-stakeholder model of internet governance as they desired a multilateral form of state-centered governance rather than a distributed multi-stakeholder management. NGOs that advocate the market model, along with large sector representatives in the field of informatics, were disturbed as they knew that they would lose power in the new governance model: many representatives in the industry had come together as a joint bloc to oppose what they perceived as an ITU takeover of internet governance.

China proposed the strengthening of the government's role in the global internet governance in the Internet Governance Forum (IGF) and the World Summit on the Information Society (WSIS). Moreover, it suggested the creation of an intergovernmental organization under the United Nations in which governments would have the dominant position in the global internet governance, whereas civil society, NGOs, and private sectors would play the advisory role.[79]

It is also noteworthy to emphasize that China has also actively displayed diplomatic acts to export its internet norms to other countries. In 2019, in Geneva's UN district, Huawei, the Chinese telecoms giant, has proposed a new IP, a new internet infrastructure in which nation-states would have the power rather than individuals.[80] One of China's remarkable policies in recent years is organizing promotional seminars on censorship and surveillance systems on the internet and in cyberspace, and hosting media officials from many countries for this purpose. The Beijing administration is following a steady line in providing telecommunications equipment, advanced facial recognition technology, and data analysis equipment and tools to various governments that are defending similar policies.[81]

4. THE INTERNET AND CYBER POLICIES IN THE MIDDLE EAST

4.1. History of the Internet in the Middle East and Some Descriptive Statistics

When we talk about the penetration of the internet in the Middle East it should be noted that there are wide differences in their economies, societies, and access to modern technologies and infrastructure. In the beginning, there was a rapid growth in the use of the internet in the middle of 1990s as the governments of the Middle East were unaware of the potentially negative and positive effects of internet. The timeline for first access to the internet in the Middle East (see Table 2) was by Israel in August 1984, when the Inter-University Computing Center (IUCC, also known by its Hebrew acronym, MACHBA) connected to EARN, the European Academic Research Network. As in all other geographical areas, the development of the internet in the Middle East countries has progressed largely depending on the scope and nature of their telecommunications infrastructure. In 1991, Tunisia became the first Arab country in the Middle East to connect to the internet. Kuwait established its internet service in 1992 as part of its reconstruction projects in the aftermath of the post-Iraqi invasion. Syria had only two ISPs in 1997: the Syrian telephone company and the Syrian Computer Society. Again, it should be highlighted as an important note that, except for the first introduction of the internet in Middle Eastern countries, the process of mass popularization had to take another decade. In other words, mass access of ordinary people to the internet in Middle East society only occurred in the early 2000s.

As can be seen in the Table 3 below, the 5-most populous countries in the Middle East are Egypt (102,3 million), Iran (83,9 million), Algeria (43,8 million), Iraq (40,2 million), and Morocco (36,9 million). Some noteworthy country characteristics are such that Saudi Arabia is the only country in the Middle East region that sits in the G-20 grouping. It is the largest economy in the Arab World. In terms of internet penetration rate small and ultra rich Gulf nations (Kuwait, Qatar, UAE, Bahrain) reach near

Table 2: Year of First Internet Access

Country	First Access Year	Country	First Access Year
Israel	1984	Jordan	1994
Tunisia	1991	Bahrain	1995
Kuwait	1992	Yemen	1996
Egypt	1993	Qatar	1996
UAE	1993	Syria	1997
Iran	1993	Iraq	1998
S. Arabia	1994	Libya	1998

Source: Allagui, 2020; Kalathil&Boas, 2010[82] Warf, 2007[83]

universal penetration rates. On the other hand, in all other remaining countries a significant proportion of people has access to the internet, especially young, educated, urban masses. In terms of the penetration rates, the 5-lowest performing countries are generally war-torn societies of Yemen (26,5%), Syria (43,5%), Egypt (48%), Iraq (52,9%), and Algeria (58%).

The TV Channel Al Jazeera and its website have reached a large global audience; however, apart from this, the majority of the visitors of the Middle Eastern websites are from the Arab countries in the region. The people of countries with large populations such as Saudi Arabia and Egypt also have the highest visitor status.[84] The concept of the Arab World has been criticized in many academic platforms due to the lack of real correspondence and the highly heterogeneous structure of the region; this concept may not have a counterpart in the political world, but certainly in terms of social media and cultural exchanges, Arab people in the Middle East seem to interact intensely on the same platforms. For example, Egyptians, Tunisians, Moroccans or Saudi Arabians visit Lebanon-based websites, while Kuwaitis, Iraqis or Syrians interact with Jordanians and Algerians.[85] It is also worth mentioning that, overall, of the Gulf countries in general and in particular, Saudi Arabia is the Middle East country that has been attacked the most in terms of cyber security and is exposed to the most fraud attempts.[86]

Table 3: Internet Users Statistics in the Middle East

Countries	Population (2020 estimated) in million	Users, in Dec/2000 in thousand	Internet Usage 31-Mar-2020 in million	Penetration Rate (% Population)
Algeria	44	50	26	58 %
Bahrain	2	40	2	95 %
Egypt	102	450	49	48 %
Iran	84	250	68	81 %
Iraq	40	13	21	53 %
Israel	9	1270	7	81 %
Jordan	10	127	9	85%
Kuwait	4	150	4	99 %
Lebanon	7	300	6	81 %
Libya	7	10	5	74 %
Morocco	37	100	24	64 %
Oman	5	90	4	79 %
Palestine	5	35	3	66 %
Qatar	3	30	3	100 %
S. Arabia	35	200	32	92 %
Syria	18	30	8	44 %
Tunisia	12	100	8	67 %
UAE	10	735	10	96 %
Yemen	30	15	8	27 %
Total:				
Mid-East-N. Africa	463	3,994	294	70 %

Source: Internet World Stats: https://www.internetworldstats.com/stats5.htm. Numbers are rounded.

4.2. Drivers of Internet Policies in the Middle East

Governments in the Middle East have essentially formulated their national policies about internet governance at the domestic and international levels around four major issue areas, these being:

1. National security considerations
2. Other domestic priorities: institutionalization, legislation, and socio-economic development
3. Moral and societal issues
4. The bipolar interstate system and relations at the global level

In his study on cyber security and internet governance of Middle Eastern states, James Shires emphasizes that the national approach,

regulations, legislative activities and foreign policy priorities before international institutions generally occur in harmony with the Russia-China bloc. On the other hand, it appears to be close to the US-led Western bloc, with security collaborations, intelligence sharing and cooperations with IT and security corporations and private sector relations in general.[87]

According to Shires, Middle Eastern countries are following a path of keeping the gray areas wide by a conscious choice while expressing their attitude towards internal cyber security, international law and global norms on internet and cybersecurity. Another driving motif of the cyber policies of the Middle Eastern states is the regional environment of competition. As a natural consequence of the regional hegemonic struggle, disputes and low-intensity conflicts in the region, the relationship styles of Egypt, Saudi Arabia and Iran with the global system are reflected in their internet policies.[88]

This attack aimed to destroy Iran's nuclear program in cities of Buşehr and Natanz. The Stuxnet virus caused destruction of more than a thousand centrifuges enriching uranium at Natanz. According to an estimate, this cyber-attack affected Iran's nuclear program so as to delay it at least a year.

4.2.1. National Security Considerations

In 2010, Stuxnet and Flame were two significant cyberattacks on Iran. In the defense studies literature, it has been argued that the Stuxnet poses an interesting case since it was the first offensive cyber weapon to cause physical damage to an industrial facility.[89] This attack aimed to destroy Iran's nuclear program in cities of Buşehr and Natanz. The Stuxnet virus caused destruction of more than a thousand centrifuges enriching uranium at Natanz. According to an estimate, this cyber-attack affected Iran's nuclear program so as to delay it at least a year.[90]

Duqu and Flame, other forms of computer malware which are used for cyber espionage, were discovered in September 2011 and May 2012.[91] The discovery of Flame had been jointly announced by Kaspersky, the Russian antivirus firm, the Iranian national computer emergency response team (CERT) and CrySys Lab. Flame had reportedly been detected on Kharg Island, the Iranian primary oil facility.[92] It was also discovered on the Iranian Ministry of Petroleum's computers and the website of the ministry went offline for several days. Thus, Flame was supposed to be the most complex malware at the time, while, on the other hand, Duqu was related to Stuxnet.[93]

In response to the attack on its own energy sector, Iran launched an attack in August 2012 on Saudi Aramco, erasing and corrupting the hard drives of 30,000 computers.[94] 'Cutting Sword of Justice,' was described as the most destructive act of computer sabotage, against the world's most valuable company, Saudi Aramco. As a result of the attack, the data on three-quarters of Aramco's computers were erased; the group replaced all of them with an image of a burning U.S. flag.[95] It is known that a group named "Cutting Sword of Justice" took the responsibility for the attack. According to leaked information, Iran allegedly produced its own cyber-attack software Shamoon, using

reverse engineering from Stuxnet malware in its nuclear facilities.[96] According to media reports, it was said that Aramco may have taken about two weeks to reuse the system after the damage. The computer security research community dubbed the virus reputed to have spread across Aramco's network as Shamoon.[97]

One of Iran's most important cyber operations has been the Operation Ababil, conducted by a group known as the Cyber Fighters of Izz ad-Din al-Qassam. It launched attacks on the websites of the U.S. stock exchange and some of the USA's largest banks including JP Morgan, Bank of America, Wells Fargo, and Merrill Lynch.[98] Iran's cyberattacks "locked hundreds of thousands of banking customers out of accounts for long periods of time and resulted in tens of millions of dollars in costs to remediate."[99]

Additionally, the Iran-based Operation Cleaver has conducted major global surveillance and infiltration campaigns of key Western manufacturing, finance and security units, including the US Navy. Targets included many types of institutions such as security, energy and utilities, sea and airlines, airports, and healthcare organizations.[100] Another Iranian attack was made on a Las Vegas Casino owned by a pro-Israel and anti-Iran American citizen.[101] In March 2016, the U.S. Department of Justice indicted seven Iranian actors contracted by the IRGC who were said to have cost the American banks millions of dollars. This important cyber-attack was organised against the intranet system of the Navy Marine Corps in August 2013.[102] Iran reportedly hacked the Navy Marine Corps intranet in August 2013 and it took four months to expunge the unauthorized computer network exploitation tools from the network.[103] European executives have attempted to close down command-and-control computer servers in particular countries such as Germany, Netherlands and Britain, which may be being used by Iranian hackers linked to the Islamic Revolutionary Guard Corps (IRGC) to gather information about military and civilian officials, critical infrastructure and Iran policy, which could be crucial for offensive cyber operations in the US and several countries.[104]

The cyber realm can provide the middle powers such as Egypt, Iran and Saudi Arabia with an extraordinary asymmetric power use opportunity relevant to obtaining a more advantageous position in the power race in regional politics. It can be mentioned that there are many innovations and new tools used by the regional powers in the Middle East to consolidate their power in their own countries or to wear down the regional enemies by taking advantage of the opportunities of the information world. When we carefully follow the media and news channels, we become aware of dozens of malicious cyber campaigns and sometimes we cannot understand who the real actor is behind the scenes, while sometimes we can easily guess the track of the strong suspect. DDOS (denial of service attacks) is one of the cyber warfare methods used in the regional rivalries of the Iran-Saudi Arabia or the Iran-US struggles. These regional middle powers have also employed hackers or cyber warriors depending on the mission. There are sometimes volunteers or sometimes paid mercenaries who conduct cyber activities on behalf of governments. There are cyber patriots who conduct a series of raids or waves of state-led cyber-attacks on critics (whom they call traitors). Paid armies of trolls who aim to distort political discourse are

common in many countries. We can see Saudi Arabia's so-called cyber "flies"— ultra nationalistic defenders of state policies who often choose pictures of Saudi rulers as their avatar image. For example, Qahtani, who was dismissed over the murder of Jamal Khashoggi, is known with his nicknames as "Mr Hashtag" and "Lord of the Flies" for managing an electronic army to defend the kingdom.

Cyber-attacks have not been unidirectional. There were attacks and counterattacks. The security dilemma in the cyber domain has been working. Additionally, the scope of US cyber-attacks has not been limited to the energy field but also has included Iranian communication, electrical and defense systems. The code, known as "Nitro Zeus," has been used to hack the power grids of Tehran, which are governed by the computer systems. That sabotage plan was published for the first time by the New York Times in 2016.[105]

In May 2016, tension between Iran and Saudi Arabia in cyberspace arose. Saudi hackers defaced the webpage of the Statistical Centre of Iran. As a response, "Iran's Security Team" defaced the webpages of King Abdulaziz University and Saudi Arabia's General Authority for Statistics. Cyberattacks went on reciprocally and several websites including websites of Iran's judiciary, foreign ministry, police and cyber police forces and the Saudi Commerce Ministry were defaced. Iranian and Saudi hackers engaged in a "tit-for-tat hacker war."[106] Another example of the case of tit-for-tat cyber competition is the cyber attack on the Qatar news agency in May 2017. It has been reported that fabricated news about the Emir of Qatar was placed on the website of the Qatar news agency with the cyber attack. According to the fake news, the Emir of Qatar was developing friendly relations with Iran and Israel. The source of this violation was found to be a Russian free operation, while the Russian government denied any intervention. It remains unclear on whose behalf the hackers were acting. [107]

According to a claim, the June 2017-GCC split was related to the fabricated text credited to the Qatar's national news agency and there are allegations that this cyber operation was conducted by agents working for the UAE. It is also argued that the state of Qatar may have a counter reply to the leak of private emails of the UAE ambassador to the United States. Finally, as part of the ongoing dispute between Canada and Saudi Arabia, Israeli-produced spyware has been detected on the phones and other electronic devices of Saudi dissidents in Canada, and the operation is estimated to be controlled by the Saudi government. It is noteworthy that cyber attacks were carried out against members of the media, journalists, dissidents and elite members of civil society, especially in Saudi Arabia and Egypt.[108]

While those unconventional cyber wars were going on in the Middle East, large IT Corporations were happy with the new cybersecurity market. Private corporations in Western countries supply a wide variety of cybersecurity products and services along with consultancy services to the public and private institutions of the Middle East.[109] The widespread sale of censorship and surveillance technologies in the Middle East has been part of a broader trend by Western companies of marketing and selling network management and security products, providing customers with technological solutions for internet blocking or surveillance.[110]

Table 4: Some Examples of the Export of Surveillance Technology

Company	Technology	Exporting Country	Importing Countries
Blue Coat	Deep Packet Inspection	United States	Syria, Bahrain, Jordan, Kuwait, Lebanon, Saudi Arabia, UAE, Qatar, Iraq, Palestine, Sudan
NSO Group	Pegasus (spyware)	Israel	Saudi Arabia, UAE, Bahrain, Morocco
Hacking Team	RCS, Crisis, DaVinci (spyware)	Italy	Morocco, Saudi Arabia, Egypt, Oman, UAE, Sudan, Bahrain, Lebanon
Area SpA	Monitoring center	Italy	Egypt, Syria
Gamma International	FinFisher Suite (spyware)	United Kingdom, Germany	Bahrain, Morocco, Egypt, Jordan, Lebanon, Saudi Arabia, Oman, Qatar, UAE
Trovicor	Monitoring center	Germany	Oman, Bahrain, Tunisia, Yemen, Egypt, Syria
Nexa / Amesys	Monitoring center	France	Libya, Egypt
Sandvine	PacketLogic (Deep Packet Inspection)	Canada	Egypt

Source: TIMEP Brief-Export of Surveillance to MENA Countries[111]

In 2005, for example, as mentioned above, the US-based Boeing-subsidiary Narus signed a multi-million dollar agreement with the Egyptian company Giza Systems, licensing the deployment of their broad array of network management products across the entire Middle East region including licensing of deep packet inspection (DPI) technologies.[112] Surveillance is widespread in the Middle East.[113] A security trend that is emerging in the Middle East and across the world is malware that regimes can use to remotely access phones and computers to listen in on phone calls and read messages and this is now reflected in media reports. For example, an Israeli company allegedly sold the advanced spyware Pegasus to Saudi Arabia and the UAE, despite the lack of diplomatic ties between countries.[114]

When it was about a profitable exporting sector Western states have generally closed their eyes to democratic or anti-militaristic principles. For example, despite Germany's anti-militaristic culture and its Basic Law (Article 26), the German defense industry had turned into a major arms exporting industry by the end of the Cold War.[115] According to media sources, Germany's National Security Council approved shipments of weapons parts to countries directly involved in the war in Yemen.[116] Moreover, based on security sector statistics collected by the SIPRI:

- The United States exported 36 percent of all arms sold to the world markets in the 2014-2018 period.
- Russia became the world's second-largest exporter with a 20 percent share in the market.
- The top five arms exporters — the United States, Russia, France, Germany and China — supplied 75 percent of all weapons sold in the 2014-2018 period.
- Arms sales to the Middle Eastern countries doubled in the 2014-2018 period compared with 2009-2013.[117]

At the global level the only international export control regime is the Wassenaar Arrangement which was adopted by a United States-led group of thirty-three nations in 1996. This arrangement lists the types of technology that should be regulated, but does not contain stipulations for its enforcement. In 2013, the European Union began a process to establish an export control system, particularly referring to the importance of human rights issues. The European Commission and Parliament have been moving towards stricter export controls on surveillance technologies, but have met resistance from member states. In May 2019, Germany and other member states were reported to have prevented reform measures that would restrict export from being adopted by the EU.[118]

Since the Wassenaar Arrangement, which is the only regulatory legal system in the world, is not binding and does not have sanction power, national states make their domestic export processes in accordance with the principles of local law. The export control regime established by a few states in their own legislation is weak in terms of managing this global phenomenon and is also vague. Moreover, in a world economy where competition is painful, domestic companies and governments are often unwilling to establish new resistance mechanisms regarding their exports or to share information unnecessarily. Thus, the cyber market runs with its own rules as a dark area with a market size of billions of dollars. Implementing strict legislation and export regulation means putting oil on the bread of already very appetizing competitors. These are related to the severity of risk as the surveillance technology market continues to expand, as companies proliferate and consolidate corporate interests in maintaining an unregulated environment.

> Throughout the Middle East and, in particular, the states of Bahrain and Saudi Arabia have a very cruel and unforgiving attitude towards social media campaigns and activists for the purpose of propaganda or social organization. Similarly in Iran concerns have grown that social media is becoming a threat to national security.

The United Arab Emirates appeared in the media where it was working with a firm called Cyberpoint, which employed former American (NSA) agents to do cyber espionage. Another note in the press is that some foreign companies have set up monitoring centers in the region where governments can intercept and scan communications. The Italian company Area SpA has helped Syrian officials track citizens in real time through the establishment of such monitoring centers, and it is stated

that the company broke the European Union's sanctions regime against Syria. There is also information that the German company Trovicor has established similar listening centers in Bahrain. Firms also sell deep packet inspection (DPI) technologies to the Middle East, allowing authorities to monitor and redirect internet traffic. American company Blue Coat has provided the Syrian regime with the most advanced technical tools and information management systems to filter internet traffic. How exemplary it is to see that the human rights-centered sanctions regime of the USA or EU countries are full of holes.[119]

Throughout the Middle East and, in particular, the states of Bahrain and Saudi Arabia have a very cruel and unforgiving attitude towards social media campaigns and activists for the purpose of propaganda or social organization. Similarly in Iran concerns have grown that social media is becoming a threat to national security. The Iranian government debated about the filtering of the Telegram, one of the most popular social media platforms in Iran, calling these messengers a threat to the national security of the Islamic Republic. Iranian elites emphasized that Telegram information is used by Britain, Germany and Israel and described these nationwide protests as an example of the anti-security use of the Telegram.[120] In this respect, Chief of the Iranian Cyber Police, Kamal Hadianfar, also referred to the activities of the Telegram channel "Amad News" under the management of Ruhollah Zam, who runs a channel on Telegram that spreads messages about upcoming protests in 2017 and shared videos from the demonstration.[121]

Iran has banned the messaging application Telegram in 2018 since it was being used by groups and individuals spreading unrest in the country. Mahmoud Sadeghi, a former member of the Islamic Consultative Assembly of Iran, emphasized privacy security in response to the filtering of Telegram.[122] Recently, there has been a massive data leak of forty-two million Iranian Telegram users including their phone numbers, secret keys, user account ID's and usernames. Amir Nazemi, Head of the Information Technology Organization of Iran and a Deputy Telecoms Minister, stated that the hacking group had identified and referred this to the judiciary for prosecution.[123]

4.2.2. Institutionalization, Legislation and the Role of the Internet for Socio-Economic Development

All GCC states have long-term national plans, for example, Qatar's National Vision 2030, the Abu Dhabi Economic Vision 2030, and the most well-known being Saudi Arabia's "Vision 2030," championed by the Crown Prince Muhammad bin Salman. These national plans display three broad similarities. All these rich nations declare that they want to shift their economic base from extractive industries towards knowledge-based produciton. They also aim to reduce the role of the public sector in all areas of life. Egypt has also had many strategic plans both internally and delivered by development consultants.

Iran acknowledges the significance of information technologies and the government perceives the internet as fundamental for economic and social development. Building a communication infrastructure is among the five-year plans of the country.[124] In the global forums related to internet governance, Iran is concerned with the digital divide since 2003. Especially under the Ahmadinejad administration, Iran emphasized bridging the digital divide since it is essential for economic de-

velopment.[125] On the other hand, as a result of a great number of sanctions on Iran, the country decided to focus on its own industries rather than relying on US-built platforms in contrast to Persian Gulf Cooperation Council states. For economic development, Iran has been in cooperation with Russia in several fields. In the Middle East, it can be observed that the states, especially Egypt, Iran, the UAE and Saudi Arabia, who have tough attitudes in terms of internet governance, are facing an impasse regarding developing the national economy and society and laying the foundations of a knowledge-based economy without losing the control of the power of the state against online destructive activities.[126] In terms of the relationship between the internet and developmental economic dynamics, knowledge economy is the essential concept to be studied. Interent connectivity provides many opportunities for individuals and firms in developing countries. The internet offers unprecedented possibilities for small and mid-size enterprises. In a competitve world economy, if you offer high quality goods or services, you may reach millions of potential customers all over the world. However, there are negative side effects of technology too. Cyber attacks pose significant political and economic challenges to the rapidly developed and wealthy nations in the Middle East.[127] Financially, the Middle East seems a desirable target for many cyber criminals due to the poor awareness of many IT users, the lack of technical ability and appropriate legislation, and the availability of massive wealth.[128] As an interesting point, it has been revealed that commercial companies located in the Middle East and especially in the Gulf region suffer from cyber attacks with much greater economic losses than their peers in the rest of the world. This is because many Middle Eastern companies purchase cyber security technology to protect themselves from these attacks and losses. According to other interesting data, although the Middle East region has high internet and smartphone penetration rates compared to the world average, it has a low performance in terms of cyber education and training. [129]

Therefore, Middle Eastern governments have a new set of tasks: the obligation to prevent cyber security's potential harm to economic and social life. However, most of those nations predominantly are concerned with the political dimension of internet security. The governments of Egypt and the Gulf states appropriated the concept of cybercrime to counter political opposition. This tactic was combined with a similarly broad definition of other key legal terms such as terrorism, and strict anti-protest and media laws. This innovation is important for the global development of cyber norms because it demonstrates how states that are not "norm-takers" incorporate such norms into their practices in strategic maneuvering, signaling their alignment with the norm through national strategy documents and then deviating from the norm in their domestic laws.[130]

Moreover, the rise in cybercrime in cyberspace (internet fraud, hacking and influencing of computers and internet systems, invasion of the privacy of individuals and groups, theft of information, etc.) in Iran has led to taking legal measures such as the adoption of the Computer Crimes Law (known as the Cybercrime Law) in 2009, which was approved by the Islamic Consultative Assembly of Iran in that year (Article 19, 2013). This was to determine cases of criminal use of computer and telecommunication systems. Following the approval of this law, in accordance with article 22 of this act, a committee was established to

determine cases of criminal content. The list is divided into five chapters under "Content against public decency and morality," "Content against sanctity," "Content against public safety and security," "Content against the government and public officials and institutions," and "Content for committing cybercrimes and other crimes." (Computer Crimes Act, 2013). It was called the "Computer Crimes Law" and part of this list is also mentioned in the Islamic Penal Code. In Saudi Arabia too authorities have introduced several institution building initiatives including establishing a National Cyber Security Authority and Saudi Federation for Cyber Security and Programing.[131]

Mohammed Morsi came to power after the Arab Spring. The overthrow of Mohammed Morsi with a military coup, resulted, in fact, in the army, which ruled the country with a secret hand, again holding power, this time with more authoritarian measures after a short break.

Accordingly, the Egyptian military regime under Sisi, which came to power with the coup and pulled back from the repetition of popular movements in 2011-2012, is interested in surveillance technologies that allow internet traffic monitoring, intercepting and re-routing activities and which support ultimate state control over the internet. According to the 2014 constitution of the military regime (Article 31): "The security of the information field is an integral part of the national economic and security system. The state undertakes to take the necessary measures to protect it " (Arab Republic of Egypt, 2014). According to a recently enacted regulation by the Egyptian Parliament (approved by Parliament on June 5, 2018), social media accounts with too many followers (more than 5,000 followers) will be treated as a business-media organization. Egypt's enactment of a new cybercrime law, ostensibly aimed at combating extremism and terrorism, allows authorities to block websites considered "threats to national security" or "national economy."[132]

Arab nations came together and established a common platform to enhance cooperation so as to effectively combat cyber-crimes. The Arab League became the initiator to create the Convention on Combating Information Technology Offences (*jara'im tiqniyyat al-mu'alumat*) by the Arab League (known as the Arab Convention). In the preamble of the Arab Convention[133], it is stated that

...Desiring to enhance cooperation between themselves to combat information technology offences threatening their security, interests and the safety of their communities, convinced of the need to adopt a common criminal policy aimed at protecting the Arab society against information technology offences, taking into account the high religious and moral principles, especially the ordinances of Islamic Law (Shari'a), as well as the human heritage of the Arab Nation which rejects all forms of crimes, and having regard to public order in every State, adhering to the relevant Arab and international treaties and charters on human rights, and guaranteeing, respecting and protecting them...

Between 2011 and 2018, Saudi Arabia, Oman, and the UAE all updated earlier laws while Egypt, Bahrain, Qatar, and Kuwait implemented new laws. The legal frameworks have become much more authoritarian as the regional rivalry has increased and the world politics have become more polarized. For example, the cybercrime law in Saudi Arabia was updated in 2015 with what was termed a

"naming and shaming" clause for offenders. Similarly, the updated Omani law in 2011 has a section explicitly titled "content crimes," covering any use of ICTs to "produce or publish or distribute or purchase or possess whatever might prejudice the public order or religious values" (Government of Oman 2011). The updated UAE law in 2012 is one of the starkest examples, as Article 9 prevents almost any form of online political debate. After the Qatar crisis in June 2017, the UAE attorney general stated that showing sympathy for Qatar online would be treated as a cybercrime. In October 2018, the Saudi Public Prosecution reiterated spreading rumors in the updated cybercrime law in an oblique reference to the alleged murder of Saudi journalist Jamal Khashoggi.[134]

4.2.3 Cultural Hegemony of the West

In 1995, officials from a variety of Arab nations came together in Cairo to discuss two existential threats to national securities of Middle Eastern nations: terrorism and satellite television broadcasts. The Egyptian Minister of Information said that, "it is an extremely sensitive period because the Arab mind is subjected to infiltration by a satellite culture... this is threatening our identity and our culture."[135] In 2003, Zimbabwe President Robert Mugabe called the internet a tool of British imperialism. Iranian mullahs maintain that the West, especially the USA, aims to disrupt the basic codes of Islamic society by infusing Western culture into Iranian society by undermining the moral and Islamic values in Iran. Thus, Tehran has established consistent national policies and it is determined to resist Western cultural penetration through the internet. Supreme Leader Ali Khamenei stated that digital media is a tool of cultural infiltration and domination which led Iranian society to diverge from religious beliefs.[136]

As an example of the potentially devastating effects of social media and the internet, official media releases highlight a large number of crimes in Iran due to cyberspace. Instagram and Telegram applications are said to increase the crime rate. Chief of Iranian Cyber Police, Kamal Hadianfar, stated that they send Cyber Police 100 to 200 Telegram channels for removal daily, most of which are "porn and terrorist."[137]

With respect to that, Iranian executives argued that they would establish national social media platforms which are alternatives to foreign giants such as Facebook and Twitter.[138] For instance, Iran has established "Mehr", a social media platform, as an alternative to Youtube in December 2012.[139] Additionally, Iran had plans to create a national computer operating system based on Linux (initiated in 2012), a national email service (initiated in 2013), and a national internet, unconnected to the World Wide Web.[140]

According to officials, Iranian society does not support the social networks that the US has built. The long-term plan should not restrict or block access to social media applications and local alternative social networks and applications must be developed in order to end the domination of Westerners on these strategic tools.[141] The need to establish a "national information network" has long been emphasized in the National 5-Year Development Document. In this regard, for a long time, the issue has been raised about the need to establish regulations for the presence and activities of foreign mobile messengers. Also, Iranian authorities have long emphasized the importance of maintaining "cyber sovereignty" and establishing cyber borders.[142] With

the establishment of the "Halal Internet", the National Information Network (NIN), Iranian officials believe that the dependence of foreign (US) powers on technological products and services will decrease and thus national sovereignty in cyberspace can be fully established.[143]

4.3. The Position of Middle Eastern Countries on Global Internet Governance

Despite their many differences, Middle Eastern states have similarities with regard to internet governance at an interesting point. On the one hand, they cooperate with the Russia-China bloc in international governance platforms. On the other hand, international business relations, cyber security relations and collaborations leading in the the private sector are not creating any disturbances for both global camps. More interestingly, they cooperate with the Western camp in terms of cyber operations and intelligence sharing relations.[144] These states have developed deliberately ambiguous national cybersecurity strategies that disguise differences between domestic cybersecurity priorities and those of their international partners. Additionally these states have appropriated international norms on cybercrime, specifically the Council of Europe's Budapest Convention of 2001, in order to counter political opposition and restrict their online public spheres through new cybercrime legislation.[145]

The main international norm regarding cybercrime is the Budapest Convention on Cybercrime agreed by the Council of Europe in 2001. None of the states considered here have acceded to the Budapest Convention (accession is available to nonmembers of the Council of Europe, while signature is only available to members). As of 2020 September, there are sixty-four ratifications or signatures/accessions to the convention, only two of which are in the Middle East: Tunisia and Israel. On the other hand, the Arab Convention was signed in December 2010 by the members of the Arab League, and it has been ratified by Egypt and all GCC states other than Saudi Arabia. The Arab Convention is different in several key ways to the earlier Budapest Convention. The Arab Spring and near contemporaneous signing of the Arab Convention was the catalyst for the spread of cybercrime laws in the GCC.[146]

According to the Freedom House report, at least 36 governments (including Jordan, Egypt, Saudi Arabia) have received closed-door Chinese training on "new media and information management." Moreover, 18 countries use a Chinese network system for surveillance.[147] Iran has good relations with Beijing, and it is claimed that Iran has been making a huge effort to be supplied with internet filter software especially through China's Huawei Telecom Company.[148] Moscow and Tehran had already worked together, attending meetings of the joint working groups of ICTs and constructing several ICT projects.

One of the most controversial gatherings was the NetMundial meeting in 2014. This big internet-governance forum was held in São Paulo on April 23rd-24th and brought together more than 1,200 participants from 97 countries to assess global internet governance matters in the aftermath of the Snowden leaks.

Iran attended the Netmundial meeting under the presidency of Rouhani.[149] It shows that Iran promotes the idea that, not only governments, but also civil actors should discuss the internet governance issues, showing its commitment to "multi-stakeholderism" in an international meeting.

It is useful to note the perspective of two major states: Germany and Brazil. Both had clearly outlined their thoughts in anger of being surreptitiously monitored by the US intelligence agency with technical surveillance. Brazilian President Dilma Rousseff spoke of the importance of finding alternatives to America-based internet services. Chancellor of Germany, Angela Merkel, also expressed her opinion on separating from the world internet and establishing a separate European internet. Both expressed their discomfort with the news that the American National Security Agency was spying on their emails, among other things. Governments in Brazil and Germany sponsored a UN General Assembly resolution on privacy rights, officially adopted on 18 December 2014.[150]

5. CONCLUDING REMARKS

Cyberspace is a global domain in which interdependent networks of information systems and infrastructures including communication networks, computer systems, and the internet exist. In cyberspace, nation-states have different norms and values and divergent opinions regarding the global governance of networks due to their political and social considerations. Cybersecurity is a significant issue for nation-states as they are exposed to many offensive and sophisticated external cyber-attacks, cyber-espionage, and surveillance practices from each other. Contemporarily, the issue in the global internet governance is not related to technical coordination but the problem of cooperation.

According to liberal institutionalist theorists such as Joseph Nye, internet governance is actually part of the problem-solving process of rational states that are concerned with expanding the possibilities of cooperation in complex interdependence. The necessity for collective action in the internet space should be understood as an element embedded in rules, institutions and processes in the management of policy areas such as trade, security, development and intellectual property.[151] However, the competitive cyberspace environment inevitably brings about tensions among nation-states. It is even interesting to note that, within the same domestic context, there might be diverging interests, ideas and perceptions.

The dispute between the US-led Western camp and the Eastern camp reflects that nation-states are not reaching compromise about the future of global internet governance and associated norms. The Eastern camp predominantly argues that existing international law does not cover cyberspace so there is a need for a new convention and advocate for state-led internet governance rather than multistakeholder governance. As these camps, especially the US and China, mostly have different interests in every field. Competing rules and interests of these also have surfaced around the international internet governance institutions.

In an environment of deep competition between the United States and China-Russia bloc - the European Union prefers to be positioned somewhere in the middle of the two sides.[152] Many governments are also dissatisfied with US dominance over the internet and internet governance institutions. On the other, US dominance is not only criticized by authoritarian states but also from voices against the US 'digital colonialism' and 'military-digital complex' coming increasingly from European parliamentarians and entrepreneurs.

A worldwide recommendation applies to Middle Eastern countries as well. Developing countries are in the process of controlling and eliminating the possible negative effects of the internet on sovereignty and national security on the one hand, and, on the other hand, are on the way to developing their own societies and national economies and modernizing them. They feel the need to balance its character. Finding the optimum balance in these two main parameters will continue to be a necessary challenge for governments, as technology attracts and uncertainties increase.

We are on the eve of entering a new phase in world politics with the American Presidential election. With the USA led by Joe Biden focusing its attention on the Asia Pacific region, it is not difficult to guess that the Middle East Region is pregnant with new developments.

For 20 years, there has already been a multipolar world politics in the emerging power hierarchy. There are breaks in state-society relations all over the world; with the Arab Spring, there are state, sovereignty and social organization dynamics that are under reconstruction.

A scattered struggle of a social front against globalization around the world shows itself in places in the Middle East. In many places, including Iran, Iraq, Tunisia, and Lebanon, the public demands more transparent and fair governance. In the light of all these developments and taking into consideration the world order with its process of change, it is very important to show a portrait of how a certain policy area (internet governance) is formed in a certain geography (Middle East). In this report, we have aimed to be able to take a meaningful photograph and make a small contribution to the field in the global policy domain that has been transformed with the perspective of the International Relations discipline.

ENDNOTES

1 Joseph Nye. 2014. The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance Paper Series Paper no. 1 https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities

D. Broeders & B. Van den Berg. 2020. "Chapter 1: Governing Cyberspace: Behavior, Power, and Diplomacy" In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

2 Andrew F Cooper & Daniel Flemes (2013) Foreign Policy Strategies of Emerging Powers in a Multipolar World: an introductory review, Third World Quarterly, 34:6, 943-962.

3 Ibid.

4 XinhuaNet News Channel "China's digital economy reaches 27.2 trillion yuan," Retrieved September 30, 2020, from http://www.xinhuanet.com/english/2018-11/08/c_137592289.htm

5 Statista Web Site, (2020). Retrieved November 18, 2020, from https://www.statista.com/statistics/617136/digital-population-worldwide/;Columbus, L. (2020). "2020 Roundup Of Cybersecurity Forecasts And Market Estimates,"

Retrieved July 09, 2020, from https://www.forbes.com

6 Ibid.

7 D. Broeders & B. Van den Berg. 2020. "Chapter 1: Governing Cyberspace: Behavior, Power, and Diplomacy" In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

8 J. Nye, 2014.

9 M. Murgia & A. Gross (2020, March 27). Inside China's Controversial Mission to Reinvent the Internet. Financial Times. Retrieved August 07, 2020 from https://www.ft.com

10 J. Nocetti, (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, *91*(1), 111-130; R. J. Deibert & M. Crete-Nishihata (2012). Global Governance and the Spread of Cyberspace Controls. *Global Governance: A Review of Multilateralism and International Organizations*, *18*(3), 339-361;

M. Finnemore & Duncan B. Hollis. "Constructing norms for global cybersecurity." *American Journal of*

International Law 110.3 (2016): 425-479.

11 J. Shires. 2020. "Chapter 10: Ambiguity and Appropriation: Cybersecurity and Cybercrime in Egypt and the Gulf" In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield, P. 205.

12 Broeders & Van den Berg, 2020.

13 S. Bradshaw, L. Laura, F. Hampson, E. Jardin, & M. Raymond. (2015, February 9). The Emergence of n Contention in Global Internet Governance. Retrieved September 02, 2020, from http://web.isanet.org/Web/Conferences/New Orleans 2015/Archive

14 Deibert & Crete-Nishihata, 2012; Nye, 2014

15 Nye, 2014.

16 D. North. 1990. Institutions, Institutional Change, and Economic Performance. *New York*.

17 Broeders & Van den Berg, 2020.

18 Deibert and Crete-Nishihata, 2012.

19 Ibid.

20 Nocetti, 2015.

21 Deibert and Crete-Nishihata, 2012.

22 G. Baram & H. Menashri (2019). Why can't we be friends? Challenges to international cyberwarfare cooperation efforts and the way ahead. *Comparative Strategy, 38*(2), 89-97.

23 J. Bader. (2019). To Sign or Not to Sign. Hegemony, Global Internet Governance, and the International Telecommunication Regulations. *Foreign Policy Analysis*, *15*(2), 244-262.

24 C. Cuihong. (2018). China and Global Cyber Governance: Main Principles and Debates. *Asian Perspective, 42*(4), 647-662.

25 Nocetti, 2015.

26 S. Golkar. (2011). Liberation or suppression technologies? The Internet, the Green Movement and the regime in Iran. *International Journal of Emerging Technologies and Society*, *9*(1), 50.

27 Ibid.

28 Murgia & Gross, 2020.

29 Nocetti, 2015.

30 Deibert and Crete-Nishihata, 2012

31 Broeders&Van den Berg, 2020.

32 The Guardian, April 24, 2014.

33 Nocetti, 2015.

34 The Guardian, April 24, 2014.

35 IANA (Internet Assigned Numbers Authority): Root Servers. Retrieved September 21, 2020, from https://www.iana.org/domains/root/servers

36 Nocetti, 2015.

37 Goel, 2020.

38 Nocetti, 2015

39 G. Bahgat. (2020). Iran and Its Neighbors Face Risks and Opportunities in Cyber Security. Orbis, 64(1), 78-97.

40 M. Finnemore & K. Sikkink (1998). International norm dynamics and political change. *International Organization*, 887-917; T. Risse-Kappen, T., Ropp, S. C., & K. Sikkink (Eds.). (1999). *The power of human rights: International norms and domestic change* (Vol. 66). Cambridge University Press; L. Adamson (2019). Let Them Roar: Small States as Cyber Norm Entrepreneurs. *European Foreign Affairs Review*, *24*(2).

41 M. M. Manjikian (2010). From global village to virtual battlespace: The colonizing of the internet and the extension of realpolitik. *International Studies Quarterly*, *54*(2), 381-401.

[42] Deibert & Crete- Nishihata, 2012.

[43] Broeders&Van den Berg, 2020.

[44] GCSC. 2019. *Advancing Cyberstability*. Final Report of the Global Commission on the Stability of Cyberspace, November 2019.

[45] M. A. Lemley & L. Lessig. (2020). The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era

[46] Ibid.

[47] Deibert and Crete-Nishihata, 2012.

[48] Manjikian, 2010: p. 395.

[49] Deibert and Crete-Nishihata, 2012.

[50] Ibid.

[51] Ibid.

[52] Clarke & Knake, 2019.

[53] Murgia & Gross, 2020.

[54] Nocetti, 2015.

[55] Baram & Menashri, 2019.

[56] Deibert & Crete- Nishihata, 2012.

[57] M. Michaelsen. (2018). Transforming Threats to Power: The International Politics of Authoritarian Internet Control in Iran. *International Journal of Communication (19328036)*, *12*.

[58] R. Safshekan. (2017). Iran and the global politics of internet governance. *Journal of Cyber Policy, 2*(2), 266-284.

[59] Cuihong 2018.

[60] Nocetti, 2015.

[61] V. Akimenko & K. Giles. (2020). Russia's Cyber and Information Warfare. Asia Policy 27(2), 67-75.

[62] Ibid.

[63] Nocetti, 2015.

[64] M. Carr. (2015). Power plays in global internet governance. *Millennium*, *43*(2), 640-659.

[65] Ibid.

[66] Safshekan, 2017.

[67] UNGA. 1999. A/RES/53/70 *Developments in the Field of Information and Telecommunications*

in the Context of International Security. New York: UN; UNGA. 2010. A/65/201 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: UN; UNGA. 2013. A/68/98 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: UN; UNGA. 2015. A/70/174 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: UN.

[68] Z. Homburger. (2019). The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace. *Global Society, 33*(2), 224-242.

[69] Broeders&Van den Berg, 2020.

[70] Broeders&Van den Berg, 2020, p. 3.

[71] Goel, 2020.

[72] Nocetti, 2015.

[73] Homburger, 2019.

[74] S. McKune. (2017, July 18). Analysis of International Code of Conduct. Retrieved July 04, 2020, from https://citizenlab.ca/2015/09/international-code-of-conduct/

[75] Homburger, 2019.

[76] Ibid.

[77] Deibert and Crete-Nishihata, 2012.

[78] Homburger, 2019.

[79] Cuihong, 2018.

[80] Murgia & Gross, 2020.

[81] Goel, 2020

[82] S. Kalathil and T. C. Boas. (2010). *Open networks, closed regimes: The impact of the Internet on authoritarian rule*. Carnegie Endowment.

[83] B. Warf and P. Vincent. (2007) "Multiple geographies of the Arab Internet." *Area* 39.1: 83-96.

[84] I. Allagui (n.d.). Multiple Mirrors of the Arab Digital Gap. Retrieved September 02, 2020, from https://www.globalmediajournal.com/open-access/multiple-mirrors-of-the-arab-digital-gap.pdf

[85] Allagui, 2020

[86] Bahgat, 2020.

[87] J. Shires, 2020.

[88] Ibid.

[89] M. Eisenstadt. (2016). *Iran's Lengthening Cyber Shadow*. Washington Institute for Near East Policy. Retrieved August 04, 2020, from https://www.washingtoninstitute.org

[90] Ibid.

[91] Bahgat, 2020.

[92] C. Bronk & E. Tikk-Ringas. (2013). The Cyber Attack on Saudi Aramco. *Survival, 55*(2), 81-96.

[93] Pahlavi, P. and Ouellet, E. (2019). "Iran: Asymmetric Strategy and Mass Diplomacy." Journal of Strategic Security 13, no. 2: 94-106.

[94] Eisenstadt, 2016.

[95] S. Jones. Cyber warfare: Iran opens a new front, (2016, April 26). *Financial Times*. Retrieved August 07, 2020, from https://www.ft.com/

[96] Finnemore&Hollis, 2016.

[97] A. B. Darıcılı (2019). Analysis Of Iran's Cyber Security Strategy With Regard To The Attack And The Defense Capacity. *Social Sciences*, *14*(3), 409-425.

[98] Jones, 2016; Darıcılı, 2019.

[99] F. Rezaei, 2019. Iran's Military Capability. *Insight Turkey*, *21*(4), 183-216.

[100] Goel, 2020.

[101] Darıcılı, 2019.

[102] Ibid.

[103] Eisenstadt, 2016.

[104] Eisenstadt, 2016.

[105] Sepahvand, 2019.

[106] Eisenstadt, 2016.

[107] Bahgat, 2019.

[108] Shires, 2020.

[109] Shires, 2020.

[110] J. A. Kerr. 2016. *Authoritarian management of (cyber-) society: Internet regulation and the new political protest movements*. Diss. Georgetown University.

[111] TIMEP: Tahrir Institutte for Middle East Policy. Retrived September 29, 2020. https://timep.org/

[112] Ibid.

[113] Elissa Miller, 28 Aug 2018, "Egypt leads the pack in internet censorship across the Middle East. Retrieved 25 September 2020: https://www.atlanticcouncil.org/blogs

[114] TIMEP: Tahrir Institutte for Middle East Policy. Retrived September 29, 2020. https://timep.org/

[115] Alexandra Sakaki, Hanns W. Mauli, Kerstin Lukner, Ellis S. Krauss, Thomas U. Berger. 2020. Reluctant Warriors: Germany, Japan, and Their U.S. Alliance Dilemma. Washington DC: Brookings Institution Press, p. 17.

[116] Deutsche Well, https://www.dw.com/en/arms-exports-germany-trails-us-as-worlds-fourth-largest-supplier/a-47847393

[117] Ibid.

[118] TIMEP: Tahrir Institutte for Middle East Policy. Retrived September 29, 2020. https://timep.org/

[119] TIMEP: Tahrir Institutte for Middle East Policy. Retrived September 29, 2020. https://timep.org/

[120] BBC News. 15 June 2017. How BAE sold cyber-surveillance tools to Arab states. Retrived 15 September 2020:

https://www.bbc.com/news/av/world-middle-east-40281963

[121] BBC News. 2 January 2018. Iran protests: Why is there unrest? Retrived 15 September 2020:

https://www.bbc.com/news/world-middle-east-42544618

[122] The Ban on Telegram. https://iranwire.com/en/features/5290

[123] Pars Today, 1 April 2020. 'Iran to prosecute hackers who leaked Telegram users' data' https://parstoday.com/en/news/iran-i119022

[124] Michaelsen, 2018.

[125] Safshekan, 2017.

[126] Bahgat, 2020.

[127] Bahgat, 2020.

[128] Ibid.

[129] Ibid.

[130] Shires, 2020.

[131] Bahgat, 2020.

[132] Miller, 2019.

[133] Arab League, (2010). Arab Convention on Combating Information Technology Offences. http://www.lasportal.org/ar/legalnetwork/Pages/typicalarablaws.aspx

[134] Shires 2020; TIMEP, 2020.

[135] Wheeler, 2017

[136] Michaelsen, 2018

[137] BBC News, 2018

[138] American Foreign Policy Council, 2013; Darıcılı, 2019.

[139] Darıcılı, 2019.

[140] Eisenstadt, 2016.

[141] Bahgat, 2020

[142] (Islamic Azad University News Agency, N.D.).

[143] Bahgat, 2020

[144] Shires, 2020.

[145] Shires, 2020.

[146] Shires, 2020.

[147] Clarke & Knake, 2019

[148] Darıcılı, 2019

[149] Safshekan, 2017.

[150] Bradshaw et al. 2015.

[151] Nye, 2014.

[152] Broeders & Van den Berg, 2020.

ORTADOĞU ETÜTLERİ

MIDDLE EASTERN STUDIES

Peer-Reviewed Political Science and International Relations Journal

ORSAM Publishes

Middle East Analysis and Middle Eastern Studies as periodical journals. Middle East Analysis, which is published bimonthly in Turkish, covers the expert opinions on contemporary developments in the Middle East. Middle Eastern Studies is a semi-annual journal on international relations. As a scholarly and refereed journal, published in both Turkish and English, Middle Eastern Studies is composed of the contributions of academics who are experts in their field. Middle Eastern Studies, where respectable, national and international level academics publishes their papers, is indexed by Applied Social Sciences and Abstracts (ASSIA), EBSCO Host, Index Islamicus, International Bibliography of Social Sciences (IBBS), Worldwide Political Science Abstracts (WPSA).

Ortadoğu Araştırmaları Merkezi • Center for Middle Eastern Studies • مركز دراسات الشرق الأوسط

ORSAM

Mustafa Kemal Mah. 2128. Sok.
No:3 Çankaya/Ankara

+90 (850) 888 15 20
+90 (312) 430 39 48

info@orsam.org.tr
www.orsam.org.tr

orsamorgtr