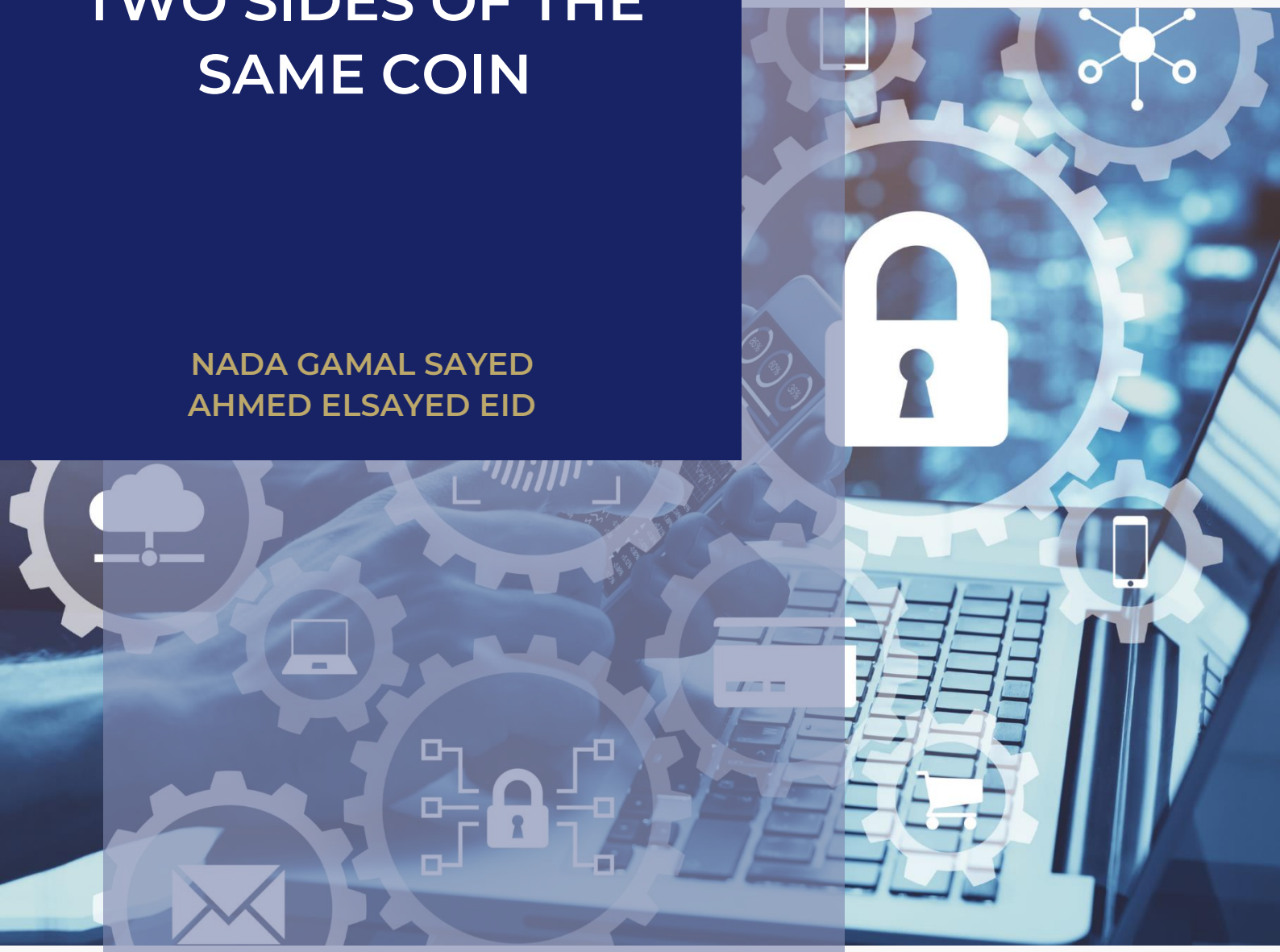
PAPER
DECEMBER 2020

UNIVERSITÀ DEGLI STUDI FIRENZE

THE PRIVATE SECTOR'S ROLE IN INTERNET GOVERNANCE: EAST AND WEST, TWO SIDES OF THE SAME COIN

NADA GAMAL SAYED
AHMED ELSAYED EID



Center for Cyber Security and International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,

Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

THE PRIVATE SECTOR'S ROLE IN INTERNET GOVERNANCE: EAST AND WEST, TWO SIDES OF THE SAME COIN

Nada Gamal Sayed Ahmed ElSayed Eid

UNIVERSITÀ DEGLI STUDI FIRENZE

Paper

December 2020

ABOUT THE AUTHOR

Nada Gamal is an International Relations post-graduate student at the University of Florence. Additionally, she is attending specialized courses in “Applied Data Science with Python Specialization” and in “Diplomacy in the Modern World” offered by the London School of Economics and Political Science. She has accomplished her “New York Model United Nations” (MUN) formation course organized by Consules. She carried out her internship at James Madison University (JMU) in Florence managing the MUN Simulation set up jointly with the University of Florence and has been invited several times by JMU to deliver lessons concerning confrontations between the European and American education system, with a particular focus on the Erasmus program. At the moment, she collaborates with the Center for Cyber Security and International Relations Studies (CSSIRS) of the University of Florence.

THE PRIVATE SECTOR'S ROLE IN INTERNET GOVERNANCE: EAST AND WEST, TWO SIDES OF THE SAME COIN

Introduction

Since 1969 human beings have witnessed the evolution of the Internet, one of the greatest revolutions in multiple fields (Van Puyvelde and Brantly 2019, 72). Despite its brief history (Nye 2011, 122), it has exponentially shaped our national politics, economies and social life (Bradshaw et al. 2014). Our never-ending dependence on its infrastructures for basic functions raises international political concerns about its growth, security and stability (Raymond and DeNardis 2013). Global negotiations around Internet governance have witnessed considerable power struggles (Carr 2015, 641). Madeline Carr explained the issue by stating that "Internet governance is mired in politics, interests, and contested legitimacy [...] because the Internet is a mechanism for the projection of power [...] and a Gramscian conception of hegemonic power through the ability of those dominant actors to set the agenda and the parameters within which global Internet governance can be considered and developed" (Carr 2015, 643). These contentious, however, were not persistent in its early days, when the Internet was self-regulated (Nye 2014) but still under the hegemonic control of the US, precisely the US Department of Commerce and technical community, thus the site of its emergence (Pires 2008, 2-3). At the beginning, the question of its management was relatively primitive since the Internet was used by a limited and a known number of users, mostly belonging to the academic and technical field, to the point that no authentication layer of code was needed (Nye 2014, 6). This initial laissez-faire system was effective in terms of innovation and prosperity (Nye 2014, 6)[1], but soon, with Internet's proliferation and commercial use, it turned into a double-edged sword, entailing new forms of

[1] Ideological libertarians proclaimed that "information wants to be free", presenting Internet as the end of government control, even though, this did not happen in reality where controls continued to persist.

misuses and attacks (Baird and Verhulst, 2004, 1-2)[2]. The rapid change of its original aims led governments to spell out the urgency of a concrete form of governance in the early 2000s (Carr 2015, 643). Both the decentralized nature of the Internet and its interconnectivity dictated the need for a new global multi-sectoral model of Internet governance (Baird and Verhulst, 2004, 2-4)[3]. This model has been formalized in occasion of the World Summit on the Information Society (WSIS) which came up with the establishment of the following definition "it is the development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet" (Van Puyvelde and Brantly 2019, 72). Nye defined Internet governance as a "regime complex composed of a loosely coupled set of regimes" (Nye 2014). This complex regime, on a spectrum of formal institutionalization, "is intermediate between a single legal instrument at one end and fragmented arrangements at the other" (Nye 2014, 7-9). DeNardis, instead, talked about a system "of administrative and technical coordinating tasks necessary to keep the Internet operational and to establish related public policy" (DeNardis 2016). Once again, DeNardis stated that these tasks range from "technical standard setting and the administration of domain names and numbers to setting policies related to cyber security and privacy" (Raymond and DeNardis 2015). Many of these tasks are carried out only by the private sector (Raymond and DeNardis 2015)[4]. In this regard, Madeline Carr stressed that the private-sector-led multistakeholder approach tends to strengthen the "existing power relations rather than disrupt them" (Carr 2015, 642). Part of Carr's explanation relied on the fact that most of the Internet infrastructure is owned and operated by the private sector, mainly by US-based multinational companies, and that the current system is prone to the interests of advanced industrial

[2] The free-riding behavior in the form of crime, attacks and threats creates increases states' perception of insecurity and vulnerabilities.

[3] It is interesting to underline how the majority of governments (despite the different interests at stake) recognized the inefficiency of their sole involvement in Internet governance and considered inadequate the traditional form of governance, devised under the guise of Westphalian system. In particular, this inefficiency became clear after the early success of the Internet which, indeed, was the product of the absence of direct state's control.

[4] Raymond and DeNardis highlighted how the way Internet governance works in practice is completely different from theory: "much of Internet governance is not multi-stakeholder". Indeed, as mentioned above, there are several tasks that take place only either by governments (i.e. multilateral treaties about Intellectual Property Rights enforcement) or by the private sector. In other words, the world is not either all black or all white, but rather shades of colors ranging from white to black.

democracies, in particular of the US and its western allies (Carr 2015, 654-56). The empirical evidence seems to confirm this version, since many non-Western and developing countries are increasingly putting in doubt the legitimacy of the current Internet Governance system (Bradshaw et al. 2014). Both the highly privatized nature of governance and the lack of representativeness of non-Western countries push these states to opt for a new model of governance, namely the "multilateral" one, advocating for Internet sovereignty[5] (Carr 2015, 653) and for a greater role to be played by governments in running the Internet with respect to non-state actors (Carr 2015, 653*)*.

The purpose of this research paper is to analyze the power of the private sector in Internet governance, taking into account its legitimacy in undertaking technical decisions, some of which are political in both design and effects. The hypothesis is that the private sector takes on a remarkable role in the decision-making process. For this aim, the paper is divided into two parts: the first one, that draws on Joseph Nye's theory of diffusion of power stemming from the context of information-based world, deals with the historical involvement of the private sector in Internet governance and with its crucial role as "gatekeeper" of information. In the second one, we will observe how the behaviour of the private sector, especially big tech companies, varies in democratic and non-democratic countries.

The private sector's path in Internet governance: from the starting point to the *status quo*

The outburst of a political choice

Since the Westphalian peace, sovereign states were the main rulers of national territories and this fact was unquestioned among Western states (Bislev and Flyverbom 2005, 8). However, according to Carr, a shift in the Western thinking has occurred in the 1990's and it touched the relationship among government, private sector and civil society (Carr 2015, 455). Particularly, in the post-Cold War setting, the US government has decided to focus on investing in modern technologies, viewed as the "new source or resource of power" (Carr 2015, 455-56). The private sector became more appealing and promising, an appropriate tool to

[5] Internet sovereignty is when "internet is regarded as an extension of sovereign space rather than a global sphere" and it is viewed as the threat of a "Balkanised" Internet, in other words the threat of linking sovereign network together.

attain economic renewal and global leadership in these developing technologies (Carr 2015, 455-56). The reason could be explained through Bislev and Flyverbom's words about the Foucauldian concept of power, according to which "power is equal with resources- resources like money, knowledge, numbers and authority. Whoever has relevant resources is able to influence the conduct of things, and thus has some sort of power [...]" (Bislev and Flyverbom 2005, 7). Indeed, the private sector detains several capacities both in terms of material (huge budget in investments) and skilled-human resources (Nye 2014, 133), and it was deemed the appropriate mean to yield this new source of power and to strengthen the hegemonic position of the United States of America (Carr 2015, 456). As a consequence, in the mid-nineties the US government kick-started a process of commercialization and privatization of Internet infrastructure which was owned and operated mainly by the government itself (Raymond and DeNardis 2015). This sort of migration of power and responsibilities in Internet governance from government to the private sector, to be viewed under the lens of the "US government leading the private sector to water" and of an US political strategy, entailed the coordination of the interests of both actors (Carr 2015, 645-46). Nevertheless, time "destabilized" this harmony and unavoidable conflicts of interest came forth as soon as the two actors got to realize the power induced by the Internet (Carr 2015).

Technical and policy role of the private sector

According to Nye, in the 21st century there are two main concerns of states: the excessive online flow of information (deriving from the information revolution) and the challenge of their control (Nye 2011, 114). This information revolution (Nye 2011, 114)[6] enabled more individuals to freely get information, thus power (Nye 2011, 113-14). It follows that a new type of power has emerged, defined by Nye as "power diffusion", that favours the migration of power from states to non-state actors. This distribution of power (both vertically and horizontally), according to Nye, "will undercut the monopoly of traditional bureaucracy" and letting non-state actors to play a relevant role in world politics alongside the states witnessing the loss of control over more and more fields (Nye 2011, 114-15).

[6] Nye stated that it "is based on rapid technological advances in computers, communications, and software that in turn have led to dramatic decreases in the cost of creating, processing and transmitting, and searching for information". what is peculiar in this revolution is the huge amount of information that can be transmitted at negligible costs, therefore the lower barrier to entry too.

That's when an attempt to define the *quid* behind this diffusion of power becomes relevant for this research: only in the aftermath of Internet commercialization, therefore the involvement of the private sector, we could officially cover the diffusion of power[7].

Indeed, since the very beginning the private sector (IGP 2020)[8] has been performing key roles in Internet governance as it detains the control over most of Internet infrastructures (Carr 2015, 654; Raymond and DeNardis 2015, 589)[9], roughly 90-95% of the information exchanged on the web pass through them (Martino 2018, 68). Despite the multi-stakeholder approach, several technical tasks, with subsequent wide policy effects, can only be accomplished by the private sector (Raymond and DeNardis 2015, 585). For instance, in order to ensure the global interoperability of Internet, network operators are engaged in private contractual agreements among each other to conjoin several networks at bilateral interconnection points or shared internet exchange points (Raymond and DeNardis 2015, 593). Moreover, they carry out network management tasks and deal with security problems on their private networks (Raymond and DeNardis 2015). Some private Internet registers, such as Verisgen, control the operation of generic top-level domains (Raymond and DeNardis 2015).

Additionally, social media platforms have a relevant policy-making role while permitting citizens to access the digital public sphere. In particular, they can enact online rights (i.e. freedom of expression and privacy) through several means: they control content as they could delete/block it and they set subscriber privacy rules (DeNardis and Hackel 2015, 1-2). The power of the private sector relies on its ability to control/access/release information. DeNardis (2014, 13) mentioned some forms of "delegated" governance from governments to private entities. Related to that, media companies act as information

[7] Consider for instance the growing number of websites: in 1993, there were around 50 websites in the world and by 2000 that number had exceeded 5 million (think about the emergence of Google in 1998 and of Wikipedia in 2001 and their global effects).

[8] Here the notion "private sector" refers to: social media, and cloud and search platforms (such as Apple, Facebook, Google, Microsoft, Twitter, YouTube); Internet Access Providers (such as NANOG, RIPE, ENOG, LACNOGM APRICOT, MENOG, AfNOG) and hosting companies; domain name registries and registrars; Internet exchange points (IXPs), Internet associations (trade association of Internet firms); cybersecurity firms; copyright and trademark holders (RIAA, MPA, IFPI, INTA); cryptocurrency industry.

[9] Internet infrastructures (known also as backbones) are composed mainly of an array of networks such as fibre-optic cables, switching centers, routers and radiofrequency antennas and are located within physical boarders and subject to national laws. This means that the private sector largely controls both the physical and the virtual components of the Internet.

intermediaries that carry out tasks governments cannot accomplish via traditional mechanisms, i.e. censorship activities, surveillance systems, law enforcement and copyright (DeNardis 2014, 13). When they decide to comply or not with the governments' requests, they modify what is referred to as freedom of expression and what not, therefore they can restrict or promote civil liberties (Raymond and DeNardis 2013). Usually, the relationship between public and private actors is regulated through the "partnership principle" that enables both actors to reach common agreements and objectives (Bislev and Flyverbom 2005, 18-20; Carr 2015)[10]. However, more tensions are coming forth since they are attaining awareness of the power of the Internet (DeNardis 2014)[11]. In the aftermath of Snowden's disclosure, it was very interesting to witness the reaction of big-tech companies that were worrying "about brand damage and about the incompatibility of pervasive monitoring with civil liberties" (Bradshaw et al. 2014, 58).

The private sector is facing more challenges related to its legitimacy in fulfilling technological tasks with direct public policy formulation. The legitimacy- related matter rests on the fact that the private sector is unelected, lacking accountability and comprises a large extent of US-based companies (Carr 2015, 654). According to different scholars, its legitimacy has two main grounds: technical expertise (Bislev and Flyverbom 2005, 18) [12]and the capacity to meet the interests of civil society (Carr 2015, 655). Despite the issue of its legitimacy, most governments still deem private-sector-led multistakeholders to be the adequate model for Internet governance. A clarification to be spelled out specifies that the private sector's role as a policy-maker applies to a limited number of private companies, mostly Western firms such as Google, Facebook and Microsoft. It is evident that those companies are not representative of smaller firms or non-Western firms, but it was quite justified taking into account their market share and global reach

[10] Policy and profit objectives are attainable by means of the development of common goals and of an alignment of economic and political interests. These partnerships enable big tech companies to gain political influence in return for technical capabilities. It is an approach that privileges consensus over conflict, values over regulations. It can be seen under the lens of what Marianne Frankline termed as "manufacturing consensus" rather than coercion or it can be conceived as a form of "enrolment". Thus, it is based on a win-win approach.

[11] For example, the notion Encryption triggered several debates as it displays the site of competing values in cyberspace such as law enforcement and national security versus individual privacy and economic security.

[12] Some scholars describe the private sector approach to influence policy as a "learning approach" instead of a "lobbying approach", in other words by presenting themselves as relevant resources to Internet governance.

(Carr 2015, 655). A critical viewpoint could formulate the following question: if the involvement criteria in the decision-making process are the aforementioned, why are giant companies such as Huawei or Baidu not covering a relevant role in Internet governance?

East and West: two sides of the same coin

While approaching Internet governance, states reflect "their internal regime and position within international politics" (Van Puyvelde and Brantly 2019, 83). Therefore, we could deduce how the encounter of contrasting cultures, policies and ideologies contributes to the increasing fragmentation in Internet governance (Kolton 2017). To get to the point, if on the one hand Western countries deal with "cyber security", on the other hand authoritarian countries, i.e. China, acknowledge "Information security", which is achievable even through the censorship of content, something that could not occur in democratic countries as long as these contents are legally protected (Nye 2014).

In this sense, it is interesting to highlight the flexibility of the role occupied by the private sector as it varies in democratic and non-democratic countries. From a theoretical perspective, the confrontation appears an easy-going task, but the actual application is way more demanding. The Eastern side seems to give more credit to the Realist International Relations (IR) approach; indeed, states aim at prioritizing the role of governments to non-state actors' detriment in Internet governance (Bradshaw et al. 2014)[13]. The main concern is to guarantee political stability and national security; in so doing, non-state actors should collaborate with governments. For instance, in China the private sector must comply with the government's instruction and serve its requests. To put it bluntly, the Chinese government can exert pressures over Chinese companies to self-censor (Chin. and Changfeng 2017; Nye 2014)[14]. National interest is the only prevailing one in China (Chin and Changfeng 2017; Nye 2014). Indeed, authoritarian countries do not respond to the dilemma like the "democratic" one where the whole issue stems from the national security and privacy question. This last aspect is representative of the other side of the coin, the Western hemisphere, which seems to praise the Liberal Institutionalism IR

[13] Indeed, authoritarian countries believe that the Internet must be protected to ensure that societies still benefit from it, but at the same time societies need to be protected from what might derive from it. Therefore, massive systems of surveillance and censorship, great firewalls and protected networks are the main tools to control the flow of information in and outside territory.
[14] The private sector should collaborate with the government in order to ensure social and political stability and to avoid any possible threat that might trigger the stability of the regime.

approach according to which "the rational self-interest of states seeking the benefits of cooperative solutions to collective action problems" (Nye 2014, 11). As rational and utilitarian actors, both public and private sectors coordinate their actions and work on setting common and ideal goals ending up operating in a flexible and collaborative system. As argued before, some technical tasks with political impacts are accomplished merely by the private sector without the states' interference and in many cases democratic governments might ask private actors to carry out surveillance activities or block content (DeNardis 2014). However, the private sector could either comply with the government's request or ignore it (DeNardis 2014, 11)[15]. Moreover, if the power of the private sector in democratic countries is taken to its extremes, it could hinder some governmental decisions that might harm its interests and the citizens' privacy or freedom of speech[16].

That being said, the complex East-West relationship and the ongoing issue-trust are no longer unexpected (Nye 2014; Herzog 2016)[17]. The clash became evident in the aftermath of Edward Snowden's surveillance revelation, according to which the US National Security Agency (NSA), with the aid of several social media platforms, such as Facebook, Google, Microsoft and Yahoo, was collecting information and private data of tens of millions of Americans (DeNardis 2016). Many countries, such as China and Iran, claimed their concerned after seeing how those big tech companies serve the US government and they understood the highly privatized nature of Internet governance to be a tool in the interests of Western countries' disposal (Bradshaw et al. 2014). As a consequence, most authoritarian and developing countries are advocating the multilateral model, and some of them have started to develop their own Internet infrastructures to control and handle the

[15] The private sector believes that "strict laws and regulations on the free flow of information across borders implies detrimental effects on the wider economy beyond implications to industry, decreases in domestic investments and welfare losses to citizens".

[16] For instance, consider the role the private sector had in avoiding the adoption of the "Stop Online Piracy Act" and of the "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act" in the US congress in 2012. For more information about the content of these acts and the actions undertaken by the private sector (such as massive online boycott led by Internet tech companies), see DeNardis (2014, 2-6).

[17] Nye explains how this loss of trust increased after states have acknowledged the increasing militarization of cyberspace and specifically of the Internet (see, for instance, Estonia and Stuxnet cases respectively in 2007 and 2010); espionage uses, subverted encryption standards and open-source software revealed by Snowden in 2013. The Internet seems to be a medium that consents states to achieve their political purposes with less risk and costs. Therefore, tensions over Internet governance is likely to arise, advocating for a major role of states and challenging the private sector's "power".

flow of information within their national borders. For instance, Russia is looking forward to relying on sovereign information technology for critical information infrastructure, for this purpose the Russian government aims to "route Russian web traffic and data through points controlled by states authorities and to build a national Domain Name System to allow the Internet to continue working even if Russia was cut off from foreign infrastructure" (Tsydenova 2020)[18]. This threat is also perceived in Western countries. Daniel Ross, an economic officer of the U.S. department of state, stated that "telecom companies must respect rule of the law and free market enterprise and be free from political interference" (Ross 2020)[19].

In this respect, for instance, after the New Beijing National Security Act, several big tech-companies, such as Google, Microsoft and Facebook, announced their withdrawal from Hong-Kong due to the increasing controversy related to the protection of users' privacy and the high level of interference of the Chinese government through encryption and censorship system (ISPI 2020). It becomes even more interesting if we specify that the same measure has been adopted by the TikTok Chinese company. However, the US Secretary of State Pompeo declared that this app shares users' private information with China, for this reason he asked for its ban in the US, together with other Chinese apps (ISPI 2020). Taking these examples to their logical conclusion, a question comes by itself: are we heading towards a concrete second model of Internet governance according to Gramscian's conception of hegemonic power?

Conclusions

As far as our hypothesis is concerned, the role of the private sector in decision-making process is incontestable (Schaake 2020)[20] when it comes to its ability to shape social and economic structures, ranging

[18] Indeed, what Russia is trying to do is to put into practice its control over the Internet within its borders and to limit any foreign interference.

[19] Daniel Ross was referring, particularly, to Huawei's conduct. Then, referring to Chinese companies, he said the following words: "Chinese companies are implicated in espionage in the Czech Republic, Poland, and the Netherlands, have allegedly stolen intellectual property from competitors in Germany, Israel, the UK, and the U.S., and are accused of bribery and corrupt practices in Algeria, Belgium, and Sierra Leone." It seems that nowadays we are facing not only technological and economic competition, but also ideological and political one.

[20] Consider, for instance, the increasing relevant role of the private sector within international sites, such as the United Nations, European Union's institutions etc., where the involvement of the private sector in decision-making process is undebatable. These tech companies are able to take technical decisions that affect the rights and freedom of all Internet users. For instance, see Mark Zuckerberg's efforts related to the adoption of a "package of regulatory initiatives on artificial intelligence, big data and digital services".

from "individual civil liberties to global innovation policy" (DeNardis 2014, 1-3). Indeed, in a domain subject to extreme technological volatility (Nye 2014) and in a world involved in an unrelenting incorporation of new technologies, the role of the private sector is crucial owing to its flexibility, adaptability and rapid management of unforeseen events. Moreover, detaining the power of either facilitating or hindering the information accessibility makes out of it a double-edged sword: a go-between info-provider at the governments' disposal (DeNardis 2014, 10), but also a tool serving the citizens' communication (Nye 2011, 120). Nevertheless, the former aspect is a source of several challenges for the private sector since it has to deal with different jurisdictions, cultural contexts, and technical environments; furthermore, it is supposed to track down a trade-off among national security, citizens' privacy and its reputation and profits (Nye 2011, 120). In fact, Internet users are increasingly losing trust in big-tech companies (Radu 2020)[21] and more governments are contesting the private sector's increasing strategic, geopolitical and policy-maker role (Jorge-Ricart 2020). Therefore, some questions rise up: where does the limit of the private sector's involvement in Internet governance lie and who establishes that limit? At the same time, global concerns arise as far as the limited number of private tech companies involved in the governance is concerned. In other words, all private actors do not matter the same (Carr 2015), and this explains why many non-Western governments and small-medium firms claim that their interests are not totally fulfilled in the current technical arrangements (Jorge-Ricart 2020). A possible explanation can be provided using Nye's words according to which "size still matters" (Nye 2011), nevertheless it is not a fully-exhaustive one, indeed we can add that both ideology/value and size play a relevant role in the involvement of actors in the decision-making process. At this point, we are in front of the two sides of the coin, and it is the side providing the private sector with such a great room of governance that is unconceivable at the eyes of non-Western countries. But, if the majority of the big tech companies involved in the Internet governance were China-based or Russia-based, would these countries be still advocating for the multilateral model?

Despite the private sector's current considerable role, Internet governance is not in a static situation and its evolution impacts technical

[21] After several reports about data breaches, the 200 Best Countries Report has conducted a survey asking people for their views on the power of the big tech companies. Almost 74% agreed upon the need to limits their powers and around 74% are worried that Internet privacy is at risk.

arrangements, thus the power arrangements as well (DeNardis 2014, 2). Therefore, facing the decline of the US hegemonic power over the Internet (Bradshaw et al. 2014) and the increasing number of Internet users in the Eastern hemisphere, for instance, in 2020 only Asia accounts for 50.3% of Internet Users Distribution in the World (Internet World Stats 2020), the questions is: how will the role of the private sector in Internet Governance develop in the medium-long term[22] and who has the ability to shape the features of this evolutive process?

According to Carr, in order to bolster the past achievements and benefits, it is important to allow a greater room for different voices and approaches. Therefore, we could wonder whether a possible future scenario would witness a more or less equal involvement of non-western big tech companies in the decision-making process? If yes, how resilient and long-lived could be this image of West-East collaboration? And if no, in case of actual fragmentation of Internet, what are the implications in terms of global growth, security and stability?

[22] For instance, it is very interesting to look at how big tech companies behave towards the Indian Internet market. The latter is expected to be the second-largest Internet market in the world. Not surprisingly, giant tech companies, e.g. Facebook, Twitter, Google, and Microsoft, are interested to invest in this market. However, the Indian government is introducing increasingly restrictive regulations that do not coincide with the liberal spirit of those companies, in particular measures that will affect how those companies collect and store data, sell products online and protect their users' privacy. See for instance the Data Protection Bill's requirement. It seems that India, the world's largest democracy, is getting closer to the Chinese model. With almost 700 million internet users today and a similar number of people yet to come online for the first time how will these foreign companies manage to behave? (Iyengar 2020)

References

Baird, Zoë, and Stefaan Verhulst. 2004. "A New Model for Global Internet Governance." In *Governance: A Grand Collaboration*, edited by Don MacLean, 58-64. New York: United Nations ICT Task Force.

Bislev, Sven, and Mikkel Flyverbom. 2005. "Global Internet Governance: What Roles do Business Play?" Paper presented at the ECPR (European Consortium for Political Research) Joint Sessions, Grenada, April 14-19, 2005. Accessed June 1, 2020. https://ecpr.eu/Filestore/PaperProposal/dba8c7a7-58e5-4ea7-9ec1-2a2ddc939baa.pdf.

Bradshaw, Samantha, Laura DeNardis, Fen Hampson, Eric Jardine, and Mark Raymond. 2014. "The Emergence of Contention in Global Internet Governance." Paper presented at the 9th Annual GigaNet Symposium, Istanbul, September 1, 2014. Accessed June 23, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2809835.

Carr, Madeline. 2015. "Power Plays in Global Internet Governance." *Journal of International Studies* 43, no. 2: 640-659.

Chin, Yick Chan, and Chen Changfeng. 2017. "Internet Governance: Exploration of Power Relationship." Paper presented at the 12th Annual GigaNet Symposium, Geneva, December 17, 2017. Accessed July 4, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3107239.

DeNardis, Laura, and Mark Raymond. 2013. "Thinking Clearly about Multistakeholder Internet Governance." Paper presented at 8th Annual GigaNet Symposium, Bali, October 21, 201. Accessed June 22, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2354377.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven and London: Yale University Press.

DeNardis, Laura, and Andrea M. Hackel. 2015. "Internet Governance by social media platforms." *Telecommunications Policy* 39, no. 9 (October): 761-770.

DeNardis, Laura. 2016. "One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation." CIGI (Centre for International Governance Innovation) and Chatham House (The Royal Institute of International Affairs) Paper series no. 38 (July). Accessed July

2, 2020.
https://www.cigionline.org/sites/default/files/gcig_no.38_web.pdf.

Herzog, Werner. *Lo and Behold, Reveries of the Connected World Internet*. 2016. Westford: Netscout. Accessed July 1, 2020. https://www.raiplay.it/video/2017/12/Lo-and-Behold-Internet-il-futuro-e-oggi-4692a9af-9b15-4519-9f18-4668aa7c7593.html.

Internet Governance Project (IGP). 2020. "What is Internet Governance?" Accessed June 30, 2020. https://www.internetgovernance.org/what-is-internet-governance/.

Internet World Stats. 2020. "World Internet Usage and Population Statistics 2020 Year-Q1 Estimates." Accessed June 27, 2020. https://www.internetworldstats.com/stats.htm.

Iyengar, Rishi. 2020. "Big Tech's honeymoon with the world's second-largest internet market is ending." *CNN Business*, February 26, 2020. Accessed July 7, 2020. https://amp.cnn.com/cnn/2020/02/26/tech/india-internet-regulation-tech-industry/index.html.

Istituto per gli Studi di Politica Internazionale (ISPI). 2020. "Hong Kong: App in fuga." Accessed July 7, 2020. https://www.ispionline.it/it/pubblicazione/hong-kong-app-fuga-26865.

Jorge-Ricart, Raquel. 2020. "Big Tech companies and States: policy or politics?" *Real Instituto Elcano*, March 2, 2020. Accessed July 6, 2020. https://blog.realinstitutoelcano.org/en/big-tech-companies-and-states-policy-or-politics/.

Kolton, Michael. 2017. "Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence." *The Cyber Defense Review* 2, no. 1 (July): 119-53.

Martino, Luigi. 2018. "La quinta dimensione della conflittualità, l'ascesa del cyberspazio e i suoi effetti sulla politica internazionale." *Politica&Società*, no. 1 (January-April): 61-76.

Nye, Joseph Samuel Jr. 2011. *The Future of Power*. New York: United States Public Affairs.

Nye, Joseph Samuel Jr. 2014. "The Regime Complex for Managing Global Cyber Activities." Chatham House. Paper series no. 1 (May). Accessed June 21, 2020. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

Pires, Hindenburgo Francisco. 2008. “Global Internet Governance: The Representation of Country Toponyms in Cyberspace.” *Revista Elecontròmica de Geografìa y Ciencias Sociales* 12, no. 270 (August). Accessed June 27, 2020. http://www.ub.edu/geocrit/sn/sn-270/sn-270-151b.htm.

Radu, Sintia. 2020. “The World Wants More Tech Regulation.” *U.S. News &World Report*, January 15, 2020. Accessed July 7, 2020. https://www.usnews.com/news/best-countries/articles/2020-01-15/the-world-wants-big-tech-companies-to-be-regulated.

Raymond, Mark, and Laura DeNardis. 2015. “Multistakeholderism: Anatomy of an Inchoate Global institution.” *International Theory* 7, no. 3 (November): 572-616.

Ross, Daniel. 2020. “Security or Competition? A False Choice.” Paper presented at the online seminar Cybersecurity Capacity-Building and Resilience: a U.S. and Italy Collaboration. May 18, 2020.

Schaake, Marietje. 2020. “Big Tech companies want to act like governments.” *Financial Times*, February 20, 2020. Accessed July 5, 2020. https://www.ft.com/content/36f838c0-53c5-11ea-a1ef-da1721a0541e.

Tsydenova, Nadezhda. 2020. “Russia proposes banning foreign IT for critical infrastructure.” *Reuters*, February 10, 2020. Accessed July 6, 2020. https://www.reuters.com/article/russia-technology-idUSL8N2AA3ZD.

Van Puyvelde, Damien, and Aaron F. Brantly. 2019. Cybersecurity Politics, Governance and Conflict in Cyberspace. Cambridge: Polity Press.

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,

Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and International Relations Studies