May 2019

ADDRESSING THE ULTIMATE FORM OF CYBERSECURITY CONTROL, A MULTIPLE CASE STUDY FOR THE 'INTERNET KILL SWITCH'

Patricia Adriana Vargas Leon
Syracuse University

Abstract

The Internet has proved its capacity to defy the nation-states' traditional borders. Facing this circumstance, governments became eager to control its infrastructure, as they did in the past with other forms of communication and they have attempted to shut down the Internet in several occasions. Academics and non-governmental organizations have focused their attention on authoritarian regimes because of the impact of Internet shutdowns on human rights. However, this extreme action of government control has also been part of the debate in non-authoritarian regimes. Thus, this dissertation contributes to the academic debate by analyzing democratic and hybrid regimes, their political discourse and concrete actions to shut down the Internet or to consider doing it. This process starts by questioning the traditional belief that democratic governments, self-defenders of the freedom as a human right, would not consider shutting down the Internet.

This dissertation is an exploratory study of the rhetoric and actual factors that enable democratic and hybrid regimes to shut down the Internet or consider doing it as part of their national security strategy. This project started by adopting a definition of what an Internet shutdown is, the government attempt to stop all Internet activity within the borders of its nation-state, also known as "Internet Kill Switch". The research design for this project carries an online data collection and a comparative case study to answer the research questions that drive this dissertation. Data collection included reputable sources and a triangulation process for validity purposes.

The process of online data collection started by developing an inclusion and exclusion criteria to select the case studies. Using the theoretical framework of the Securitization theory of the Copenhagen School, this study identified the arguments democratic, and hybrid regimes use to justify shutting down the Internet. At the same time, this project determined the audiences they try

to address and what they understand as a national security situation. Case studies include three well-consolidated democracies, U.S., U.K. and Australia, and two hybrid regimes, Russia and Venezuela. These nation-states were involved in an Internet shutdown, or their governments considered doing it under different circumstances.

To identify the political, legal and technical factors that enable a democratic and hybrid regime to shut down the Internet, this project determined specific variables to analyze. For comparative purposes, this project also incorporated two-young-democracies, Brazil and Mexico, and one hybrid regime, Turkey. These last three governments never shut down the Internet and did not consider doing it. From the comparison between regimes politically similar, this research identified similarities and differences in the factors that enable a government to shut down the Internet.

The second contribution comes from a conceptual point of view, by clarifying the differences between terms. In this regard, this study challenges the assimilation of shutting down the entire Internet with censorship episodes as if they were equal practices.

Finally, from an academic point of view, this dissertation determined that there are no substantial differences between the rhetoric and political, legal and technical factors that enable democratic and hybrid regimes to shut down the Internet.

ADDRESSING THE ULTIMATE FORM OF CYBERSECURITY CONTROL, A MULTIPLE CASE STUDY FOR THE 'INTERNET KILL SWITCH'

by

Patricia A. Vargas León

Law Degree, Pontificia Universidad Católica del Perú, 2002
M.S., Syracuse University, 2009

Dissertation
Submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Information Science and Technology

Syracuse University
May 2019

Acknowledgments

This dissertation is the completion of a great enterprise, the Ph.D. program. In that regard, and like most adventures in life, it was possible with the help of many people who supported me in different capacities and by the and by the grace of God. This is the time to say thank you to all of them.

Although the phrase "If I have seen further it is by standing on the shoulders of Giants," attributed to Isaac Newton, is often used, I think it is a good time to recall it. First, I would like to thank my advisor Professor Jennifer Stromer-Galley, for believing in my project at a critical time. She provided me with direction, support, and timely feedback on all my drafts. Moreover, I am grateful for her extraordinary patience and for her way to challenge me when it was necessary. I also profoundly thank my committee members Professors John Mathiason and Milton Mueller, who encouraged me to do this project from the very beginning. Their critique, feedback and in-depth knowledge on the subject helped me to improve my research constantly.

It was an honor to work and learn from Professor Jeffrey Vagle, to whom I also thank for serving as my external reader. I also would like to thank Professors Carlos Caicedo and Joon Park for being available and providing me with their knowledge when I needed it. Additionally, I thank Professor Park for serving as my internal reader.

Though not a part of my final committee, I would like to thank Professor Martha-Garcia Murillo, for mentoring me during the early years in the program. I also want to thank Professors Murali Venkatesh and Michelle Kaarst-Brown for their support and encouragement.

These acknowledgments will not be complete if I don't mention my colleagues and friends from the Ph.D. program and some ladies from the administrative staff. Special thanks to my friends and colleagues of the iSchool Fatima Espinoza-Vasquez, Andreas Kuehn, Renata Curty, Claudia

Louis and Norma Palomino, for their support through this journey and for reminding me that so much sacrifice will be worthy. From the staff members, I would like to thank Ellen Hobbs, Sue Nemier, Alecia Zema and Bridget Crary, for their help and support solving multiple administrative issues and their kindness in saying a prayer when my family needed it.

Outside of the iSchool, I thank the support of my friends and doctoral students Mariana Nava-Lopez, Kaira Fuentes-Viera, Sarita Bassil and Silvia Figari for their kindness making their house a home to me every time I came to Syracuse. To my friend Farzaneh Badieii, I thank for her support reminding me that, good things do and will happen.

Finally, I would like to thank my family members and friends, back in my country Perú, here in the U.S. and the rest of the world, who supported me throughout my Ph.D. studies. Thanks for their patience and kindness in the good and bad days. My brothers, Hernan and Marcos, have always been my greatest supporters in the whole adventure since I arrived in the U.S.; I will thank their support forever. My father who always encourages me to move forward despite the endless problems that lay ahead. Finally, I would like to thank my mom, the best gift the Lord could give to me. I want to thank her for everything, her love, her support, and her kindness. I am sure she will be there when I walk during the graduation ceremony.

Table of Contents

List of Figures

List of Tables

1. Introduction

In January 2011, the world witnessed how Egypt vanished from the global Internet for nine days. Although this practice seemed at the time as a unique case, it was not. Since 2005, many authoritarian regimes have executed this maneuver citing reasons of national security. As I will explain later in this document, following the Egyptian events, many academics conducted studies about authoritarian regimes that executed Internet shutdowns. At the same time, multiple sectors of the civil society have paid attention to this problem and became active monitoring Internet shutdowns in authoritarian regimes.

This research project has a different approach. It is my purpose to analyze the Internet shutdown policy from the perspective of non-authoritarian regimes, democracies and hybrids, because the issue also pertains to their agenda. Both, democratic and hybrid regimes have cited reasons of national security to consider an Internet shutdown. However, their concepts of "national security," and when and under what circumstances it affects their citizens have different connotations.

Moreover, despite the different views included in the debate, it is also important to note that democratic and authoritarian regimes also have history exercising actions to control the Internet (a practice that involves a broader scope that only Internet shutdowns). Between 1995 and 2011, there were 606 incidents of governmental control over their digital networks: 39% of the events occurred in democratic regimes, 6% in emerging democracies, 52% in authoritarian regimes, and 3% in fragile states[1] (Howard et al, 2011). As national governments found ways to

[1]Fragile nation-states are considered by having weak capacity to perform basic governance functions. They lack the ability to develop constructive relations between government and society. Fragile nation-states are also more vulnerable to internal and external shocks such as economic crises or natural disasters. The World Bank defines a fragile state as one having weak institutional capacity, poor governance, and political instability (Klausen & Humphry, 2015; Woolcock, 2014)

control, censor and govern the Internet, conceptions of a free and ungoverned Internet have been challenged.

Thus, the first chapter of this document introduces the research problem of this study, which is to investigate the causes that enable democracies and hybrid regimes to shut down the Internet, or to consider doing so. This chapter also describes the addresses limitations in the existing literature and presents the research goals, including the specific research questions this dissertation answers. Next, it offers the research approach of the study, including the challenge of a potential paradigm considering democratic systems and Internet freedom. Finally, this chapter defines the core concepts that I will address throughout this dissertation, including technical aspects and an overview of the governments that attempted shutting down the Internet.

1.1. Problem Statement

Authoritarian regimes' efforts to limit access to the Internet have captivated academic and popular attention (Bowman & Camp, 2013; Dunn, 2011; Harlow & Johnson, 2011b). Especially after the political process baptized as "Arab Spring," when Egypt (alongside with other nation-states), digitally vanished from global Internet, academic and professional research addressed the problem of the Internet shutdowns (Howard et al., 2011; ISOC, 2011; Vaughan-Nichols, 2011). However, it is less known that there has been an ongoing legal debate in democratic and hybrid regimes on the authority government leaders should have to execute an Internet shutdown in times of crisis.

As established by the literature, there are three things a government needs to interfere with communications: legal authority to act, technical capability and political power. Despite the type

of regime, political power is required to force individuals or corporations to comply, or the ability to direct forces to coerce compliance (Havyatt, 2011). In this research project, I will analyze these three critical elements to understand why consolidated democracies and hybrid regimes have shut down or have considered shutting down the Internet.

The research questions of this project address the need to understand and explain, why democracies, mostly self-determined as defenders of Internet freedom, have used or considered using mechanisms of governmental control that these governments criticized directly or indirectly in their official policy discourse. This point is important because there may be a double discourse produced by democratic regimes. On the one hand, they defend a free and open Internet, while on the other hand, their real actions and debates aim to control the Internet infrastructure and the access their citizens have to it (Crook, 2010; Harding, 2011; Opderbeck, 2012, 2013; Winder, 2011).

Acts of government control involve: (1) surveillance of specific websites or Internet users, (2) banning encryption, (3) partially censoring Internet activity, and (4) disconnecting or trying to disconnect Internet exchange points (IXPs). Democratic and non-democratic regimes have performed actions of this nature (Giacomello, 2005; Howard et al., 2011; Howard & Hussain, 2013; Price, 2015). Although shutting down the Internet could be considered a "recent" phenomenon in historical terms (since the earliest cases are from 2005), it is timely, and it seems to be occurring more frequently.

1.2. Research Questions

The specific research questions, which focus on democratic and hybrid governments, are:

RQ1: What is the global scope of the Internet shut down phenomenon?

RQ2: What justifications do democratic and hybrid regimes use to shut down or to consider shutting down the Internet?

RQ3: What are the political, legal and technical factors that enable a government to shut down the Internet?

The first question addresses the global scope of the Internet shut down phenomenon, this is, the list of nation-states that were involved in an Internet shutdown or had a debate on the subject. Therefore, the list includes nation-states that shut down the Internet or considered doing so, whether it was at a national level (in the entire territory of a nation-state) or a local (in a city or province). Thus, this dissertation aims to provide a detailed, up-to-date accounting of efforts by governments to shut down the Internet.

The second question focuses on understanding the broad and narrow arguments governments make to justify a shutdown. Prior research indicates that the political discourse of democratic regimes justifies government control over the Internet as necessary to protect what they call the critical infrastructure and to fight against cybercrime, child pornography, and computer frauds (Giacomello, 2005). Some governments also tried to explain their Internet shutdown episodes claiming the existence of an accident, although the same justification repeats more than once (Didymus, 2011; Espinoza, 2015; Gomez, 2013; Hunt, 2016).

The third research question looks closely at the structural factors that enable a shutdown or the consideration of it in democratic and hybrid regimes. By examining the legal, political, and technical forces that give rise to nation-states considering the exercise of full government control over Internet access, it is expected to identify critical factors that might differentiate hybrid regimes from democratic ones. This study also includes cases where governments have not considered or

executed an Internet shutdown to better isolate key structural factors that distinguish regimes that are inclined to exert the ultimate control of government authority as compared with those that are not.

Shutting down the Internet has been considered a remedy for different situations that threaten the national interest because the protection of the national interest guarantees the survival of the nation-state (Richards, 2012). The aim of this dissertation is examining those arguments since governments "construct" the concept of national interest and potential threats (Katzenstein, 2003). In doing a close analysis of the rhetoric produced by government leaders and policymakers, we expect to determine differences between hybrid and democratic regimes in building their arguments about national security.

1.3. Definition of Terms

This chapter will present some fundamental concepts associated with the phenomenon under study.

1.3.1. The Internet: A Network of Networks

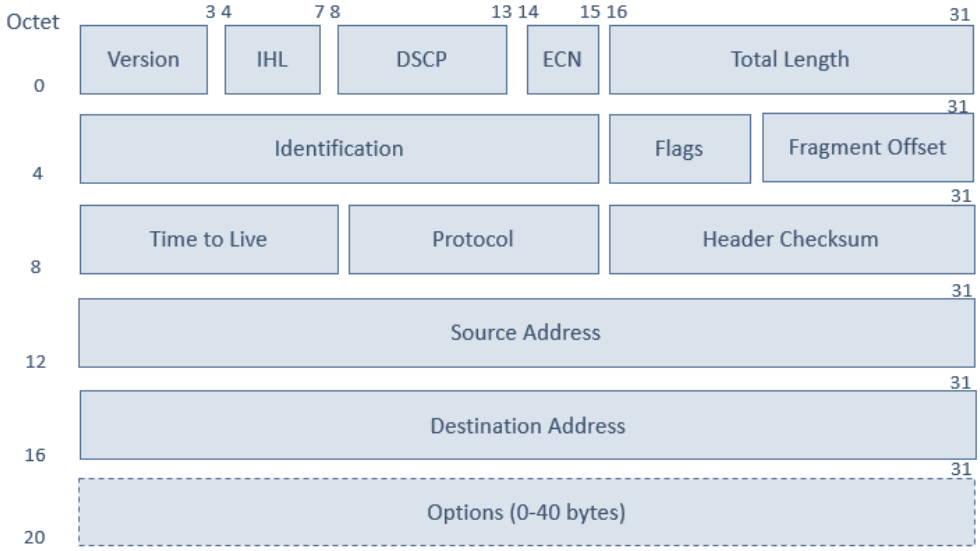
Computers are frequently connected through networks to communicate among them and to magnify their usefulness. The most widely defined example of a network is the Internet, which is a diverse set of independent networks. In this regard, the Internet is a "network of networks," and the networks that compose the Internet share a standard architecture and protocols that allow

communication within and among different constituent networks (Clark, Berson, & Lin, 2014; M Mueller, 2010). In this network of networks, the disruption of data communication should not happen, even if parts of the network go down (Subramanian, 2011).

The data that travels through the Internet breaks into small pieces called “packets”. The Internet packets travel to their destination by routers and servers, using the “TCP/IP protocol” (Transmission Control Protocol/Internet Protocol) suite. The IP protocol, in combination with several routing protocols, provides the capabilities to deliver packets to their destination in a best-effort approach; however, each packet may take a different path through the Internet (See figure 01 and 02). It is not possible to determine in advance the particular sequence of routers that will handle a packet (Clark et al., 2014)

Figure 01.-Example of an IPv4 Internet Data Packet

IP Header



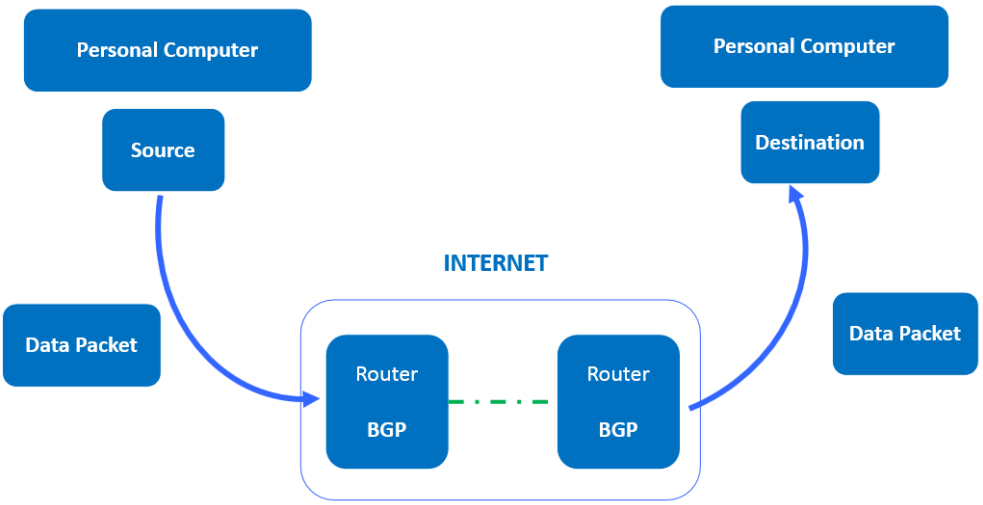
(tutorialspoint, 2019, para.2)

The elements of the packet are the following ones:

1. Version: Version no. of Internet Protocol used (e.g. IPv4).
2. IHL: Internet Header Length;
3. DSCP: Differentiated Services Code Point (Type of Service).
4. ECN: Explicit Congestion Notification; It carries information about the congestion in the route.
5. Total Length: Length of entire IP Packet
6. Identification: If IP packet is fragmented during the transmission, all the fragments contain same identification number
7. Flags: As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not.
8. Fragment Offset: This offset tells the exact position of the fragment in the original IP Packet.
9. Time to Live: Every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross.
10. Protocol: Tells the Network layer at the destination host, to which higher layer Protocol this packet belongs to
11. Header Checksum: This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
12. Source Address: 32-bit address of the Sender (or source) of the packet for an IPv4
13. Destination Address: 32-bit address of the Receiver (or destination) of the packet for an IPv4

(tutorialspoint, 2019, para.3)

Figure 02.- Travel of Data Packets' Path within the Internet[2]



Modified from Mathiason, p.8, 2009

If there is a disruption, data packets will find an alternate route and networks to reach their destination (Subramanian, 2011). In what is known as "the open architecture design of the Internet," there is not a central node (a single connection point) that controls the entire Internet infrastructure (Hiller, 2002; Mathiason, 2009; Mueller, 2002). Initially the Internet was conceived as an open communications system without ties to any organization or hierarchical constraint (Leiner et al., 1997; Subramanian, 2011). The beginning and ending points of data moving within the Internet are computers or similar devices, which are connected to the Internet through Internet service providers (ISPs) that handle the technical administrative and arrangements for connectivity. The links and routers of the Internet provide the required critical connectivity between source and destination (Clark et al., 2014).

The applications, packet-switching technology, and physical infrastructure are called "layers" of the Internet's architecture, and the most important characteristic is that different

[2] In the next chapter, there will be a more detailed explanation about the Border Gateway Protocol (BGP) and its role within the process of shutting down the Internet.

stakeholders control different layers (Clark et al., 2014; Horvitz, 2013). The lack of a centralized structure allowed the Internet "to be responsive to a very large unregulated constituency and allowing explosive growth and with increasing usefulness to its users" (Horvitz, p.6, 2013).

1.3.2. Internet Shutdown, a.k.a. 'Internet Kill Switch'

Although the lack of a centralized system of control is a resistant and resilient characteristic of the Internet, there is no guarantee that governments (either democratic or not) or any other entity won't attempt to control it (Meinrath, Losey, & Pickard, 2011). A historical analysis of the world's telecommunications history shows that one of the factors for governmental control is the existence of a national security problem, which is addressed differently in democratic and non-democratic regimes (Howard et al., 2011). In this way, governments' leaders are allowed to identify what a matter of national security is, either an enemy nation-state, malicious hackers, authoritarian regimes or human rights activists (Bobbitt, 2002; Giacomello, 2005).

When it comes specifically about an Internet shutdown, the academic literature defines this form of government control as the attempt to stop all Internet activity within the borders of the territory of a nation-state and, is colloquially known as an "Internet kill switch" (Opderbeck, 2012, 2013). The expression *"kill switch"* refers to an *"emergency-stop switch"* or just *"E-Stop"*. It also implies the existence of a single shutoff device to stop one or many activities to ensure the safety of people and machinery by delivering a concrete and predictable fail-safe response (Torzillo & Scott, 2010).

In similar terms, the expression "Internet kill switch" has been defined as a unique point of control to "shut down" the Internet and stop the transmission of the Internet packets (Economist,

2011, 2013; M. Johnson, 2011). The idea of a "switch" suggests an on-or-off state, in which access to the Internet either exists or not (Ford, 2014).

Academic and non-academic literature also define the shutting down of the Internet from three different perspectives (Economist, 2011, 2013; M. Johnson, 2011; Thompson, 2012):

1. From a political point of view, as the government's authority (or the president's authority) to disconnect commercial and private wireless networks (including both cell phones and the Internet itself) when a nation-state faces a cyber-attack,
2. From a technical point of view, as the attempt to interrupt all Internet and cellular communication activity in and out of the territory of a nation-state, when this one faces a national security threat and,
3. From a cyber-security point of view, as a control mechanism to protect the critical infrastructure when a nation-state faces a cyber-attack

Despite specific concerns about national security that governments have, and independently from any definition, it must be clear that a "kill switch device" for the Internet does not exist. This is an unrealistic vision of how government authorities could employ a physical device to disconnect computers from the global Internet. In the next section, I will explain step by step the process of how an Internet shutdown can be achieved and the elements and stakeholders involved.

Internet shutdowns are also known as *"Internet blackout," "Internet outages," "kill-the Internet power"* or *"Internet cut off"*. For this research, I will use the expression "*Internet shutdown*," because it is the most used in legal and technical documents. Any other phrase will be used as part of a citation or quotation.

1.3.3. Technical Components: Process to Shut Down the Internet

The technical process to attempt to stop the Internet is more complicated than just pressing a button (a "switch") and involves different stakeholders. Shutting down the Internet implies the interruption of transference of data packets from sender to receiver, a process controlled by the TCP/IP (Transmission Control Protocol/Internet Protocol) Protocol Suite.

Of the TCP/IP protocol suite, the Internet Protocol (IP Protocol) provides end-to-end connectivity and determines how data is formatted, addressed, routed, and received at the specified destination. The functionality of the different protocols in the TCP/IP protocol suite is organized into five abstraction layers: application, transport, Internet, network interface and physical (See figure 03) (Wood, n.d.). The layers are used to sort all related protocols according to the scope of networking involved.

Figure 03- The TCP/IP Model

The TCP/IP MODEL
Application
Transport
Internet
Network Interface
Physical

Source: (Wood, n.d.)

The technical sector and the academic community also refer to a different model called "OSI (Open System Interconnection) Reference Model," or the "OSI 7-Layer Model" that is worth to mention. This model defines seven layers that describe how applications communicate among each other while running upon different networks. The model is a generic one and applies to all network types, including (but not only) to TCP/IP, and all media types. Differently from the TCP/IP model, the OSI model contains seven layers: physical, data link, network, transport, session, presentation and application. To get a packet from an application running on device to an application running on a different device, the packets descend and then re-ascend the layers. When an application creates a packet of data to be sent; this process takes place at layer 7. As the packet descends, it is wrapped in headers and trailers, as required by the various protocols, until it reaches layer 1 and abandons the first device towards the second one. When the packet reaches second device, it re-ascends the stack, until the application layer (Briscoe, 2000).

The OSI model and the TCP/IP model are different, but they share some differences as well. The TCP/IP model is the current choice to achieve interoperability between different networks of different technology, and communities of different administrations, but back in the early 90s the academic community debated whether one model should prevail over the other one. In this scenario, it is important to point out some of the differences and similarities between both models: Both models are similar from the following points of view: Both models have a layered architecture, perform similar functions, both are protocol stack and are reference models (Rose, 1990).

When it comes to the differences, both systems have their own peculiarities:

The OSI model is a generic one, a communication gateway between networks and end-users and the TCP/IP model is based on Internet standard protocols. The transportation layers in

both models have different vulnerabilities: in the OSI model the transport layer guarantees the delivery of the packets, while the TCP/IP model doesn't provide any guarantee for the packets' delivery. Additionally, the OSI model is a reference one around which all networks are built, while the TCP/IP model is only a way of implementing the OSI model. In terms of protocols, the OSI model can fit multiple protocols, while the TCP/IP does not fit any protocol; this last distinction makes easy to replace protocols in the OSI model but in the TCP/IP model is a lot more complex problem. In a few words, the OSI model is protocol independent, while the TCP/IP model is protocol dependent (Briscoe, 2000; Rose, 1990).

Independently of the opinions of one model over the other, the TCP/IP model is the current standard for computer communications when different vendors and networks are involved.

Whoever wants to alter the transmission of the Internet packets in a particular geographic location must control at least five elements of the TCP/IP protocol: ISPS, IXPs, fiber-optic cables, all of them elements of the physical layer and, the DNS and the BGP that belong to the application layer (Beijnum, 2011; A. Chang, 2013; Eagleman, 2012; Medows, 2012). In the next paragraphs I will provide an explanation about each one of these components.

1.3.3.1. Elements of the TCP/IP Model to be Controlled to Achieve an Internet Kill Switch

The first three elements to explain belong to the physical layer of the TCP/IP model: ISPs, IXPs and Internet cables. Internet Service Providers (ISPs) are companies that connect end users and businesses to the public Internet. Therefore, they are the first thing users have in mind when they think of the Internet service. Although ISPs compete among each other, they also must

cooperate with each other to provide global Internet connectivity (W B Norton, 2001). ISPs connect to one another by creating backbones, an infrastructure known as "highway of communications". Backbones allude to large pipes that aggregate a lot of traffic (M. Mueller, personal communication, April 13, 2018).

These highways could be assimilated to the arteries of the human body that push a lot of blood (data) to our blood arteries (cities). Subsequently, those arteries feed into blood vessels (neighborhoods) and finally into tiny capillaries (individual facilities). In this way, ISPs bridge distant locations among cities, states, and nation-states (Blockmon, 2018).

By changing the configuration of the Internet and stopping the service provided by one or more ISPs, the population served by that specific ISP, which previously had Internet access, would not have it anymore. When governments try to control the Internet, they only can control national ISPs, but if an Internet user has access to a foreign connection, the national government has no control over that service provider since it is subject to a different jurisdiction (Beijnum, 2011; Medows, 2012).

In contrast, nation-states with highly interconnected networks formed by many independent ISPs are resistant to disconnection. A single cyberattack or act of disruption cannot affect at the same time the diversity of network configurations, the number of ISPs, and the number of routes out of the nation-state territory (Hewitt, 2016).

The second element to explain are the Internet exchange points (IXPs). The function of an IXP is to allow Internet networks to interconnect directly or exchange traffic between their networks (this activity is known as "peering process"[3]). In that regard, IXPs are infrastructures that

[3] Peering is a process by which two or more Internet networks connect and exchange traffic. Peering allows them to hand off traffic between each other's customers, without having to pay a third party to carry that traffic across the Internet for them. Peering is the more usual way of connecting to the Internet, in which an end user or network operator pays another network operator to carry all their traffic for them (Netnod, 2014, 2018).

facilitate the exchange of information packets among ISPs. In this context, IXPs main customers are often content providers who peer with ISPs to get their content to the Internet users. It is important to clarify that IXPs don't handle the Internet connectivity process completely and they don't provide Internet service as ISPs do. IXPs are just one of the building blocks around which the Internet is built (Netnod, 2014).

Interrupting the normal functioning of an IXP has a direct impact on the connection among ISPs and, therefore, it may slow down the Internet speed and eventually stop the Internet service (Beijnum, 2011; Medows, 2012).

Technically speaking, an IXP is an Ethernet switch, like the ones that connect computers in an office network. Each network connecting to an IXP connects one or more of its routers to that IXP's Ethernet switch, and they send traffic across the Ethernet switch to routers belonging to other networks (Netnod, 2014; Norton, 2014).

Finally, the last element of the physical layer to explain is the Internet cables. Internet cables transfer the Internet packets in and out of the territory of a nation-state. Although satellites facilitate some Internet traffic, 97 percent of global web traffic is dependent on deep-sea networks of fiber-optic cables and only 3% through satellite. Submarines cables (alongside with the Internet Exchange Points (IXPs) play a critical role interconnecting national and international networks. Currently there are approximately 213 cables all over the world, and most of them are privately owned. Lately, companies that get a profit out of Internet content (f/e Google and Facebook) are also investing in cables. However, if these companies can transport the data they produced, this activity will have an impact on the international Internet traffic. This situation would be a challenge to current governance models (Poznanski, Internet Without Borders, Blanc, Valente, & Vicentin, 2017).

Cables are not exempt from disruptions; average reports talk about 300 incidents per year. Submarine cables get cut regularly, and the cable repair industry has considerable experience dealing with these situations. Nevertheless, most of these failures are the result of accidents occurring in shallow water, and not due to deliberate actions. There is enormous capacity and resiliency among the cables crossing the ocean. Therefore, to do significant damage, a saboteur would need to take out numerous cables in short order (Madori, 2015).

Nevertheless, saboteurs do exist. The importance of the Internet cables became evident in 2008 when an unknown individual or entity cut cables that carry three-fourths of the communications between the Middle East and Europe. Accidents and similar episodes occurred in 2011 and 2013 (A. Chang, 2013; S.-I. Chang, Wu, & Cho, 2011; Eagleman, 2012). Satellites cannot replace the capacity lost due to the sabotage of one or more major submarine cables. The Internet may be able to route around breaks, but Internet routing cannot create additional capacity where none exists (Madori, 2015).

The last two elements to explain belong to the application layer, the DNS and the BGP. The Domain Name System (DNS) is a hierarchical naming system that translates the host names into Internet Protocol (IP) addresses[4]. In other words, the DNS translates human-readable domain names like "something.com," into an Internet Protocol (IP) address. The DNS exists because when an Internet user wants to access a site, that person will remember "something.com," instead of the IP addresses 22.231.113.64 or 194.66.82.11[5]. In this way, the Internet DNS is known as the "master address list" of the Internet (Vaughan-Nichols, 2011; Wang, 2003).

[4] An IP address is a number that indicates the location of a device on a network using the TCP/IP protocol. IP addresses allow data to reach the intended destination on a network and the Internet (Postel, 1981).

[5] These are examples of what is known as IPv4, IP addresses with four pairs of numbers separated by dots. Each pair is a number that can have a value of 1 to 255. IPv4 supports a 32-bit address space (Postel, 1980). Facing the exhaustion of the IPv4 addresses, the Internet Engineering Task Force (IETF) created the IPv6, which supports a 128-bit address space (Deering & Hinden, 1998).

For the DNS to function correctly, so Internet users can connect to the site they wish, the DNS must have the right address information. For this purpose, the configuration of the Internet routers on the network must allow a DNS server to send and receive data from the high level "root servers"[6] coordinated by the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Assigned Numbers Authority (IANA). By removing access of a nation-state DNS to the root servers, the DNS information will become outdated and gradually connectivity will erode (M. Mueller, personal communication, April 13, 2018).

Finally, the Border Gateway Protocol (BGP) is the routing protocol that shares the master routes of the Internet. In this way, the BGP makes it possible for ISPs to connect to each other and for end-users to connect to more than one ISP. The BGP is the only protocol capable of connecting multiple connections to unrelated routing domains. This is a critical operation for the Internet to function (Dou, Li, Qin, Kim, & Zhong, 2007). The BGP is a potential target for a cyber-attack. When the BGP does not provide routing information or does it incorrectly, the communication and routing of packets among ISPs suffer. When this situation occurs, reports say that there is an Internet shut down (Cowie, 2011a, 2011b).

[6] The root zone is a network of hundreds of servers in many countries around the world. They are configured in the DNS root zone as 13 named authorities (IANA, 2016):

a. Root-servers.net - 198.41.0.4, 2001:503:ba3e::2:30 - VeriSign, Inc.
b. Root-servers.net - 192.228.79.201, 2001:500:84::b - University of Southern California (ISI)
c. Root-servers.net - 192.33.4.12, 2001:500:2::c - Cogent Communications
d. Root-servers.net - 199.7.91.13, 2001:500:2d::d -University of Maryland
e. Root-servers.net - 192.203.230.10, 2001:500:a8::e - NASA (Ames Research Center)
f. Root-servers.net - 192.5.5.241, 2001:500:2f::f - Internet Systems Consortium, Inc.
g. Root-servers.net - 192.112.36.4 - US Department of Defense (NIC)
h. Root-servers.net - 198.97.190.53, 2001:500:1::53 - US Army (Research Lab)
i. Root-servers.net - 192.36.148.17, 2001:7fe::53 - Netnod
j. Root-servers.net - 192.58.128.30, 2001:503:c27::2:30 - VeriSign, Inc.
k. Root-servers.net - 193.0.14.129, 2001:7fd::1 - RIPE NCC
l. Root-servers.net - 199.7.83.42, 2001:500:9f::42 –ICANN
m. Root-servers.net - 202.12.27.33, 2001:dc3::35 - WIDE Project

1.3.3.2. Feasibility

As demonstrated by the experiences in Egypt and Syria, when the governments of those nation-states tried to shut down the Internet, the population found the way to regain access to the international Internet again (Dunn, 2011). Therefore, a legitimate question to ask is whether it is possible to shut down the Internet in a nation-state and thus to disconnect it from the global Internet?

The answer remains as controversial as the question. We already mentioned that the Internet is as a network of networks without a single point of control. This characteristic made the Internet famous for being "resilient" and was supposed to survive the most extraordinary circumstances (Dyn, 2014c, 2014b). Sir Tim Berners-Lee emphasized that there is not a switch-off-device for the Internet at a global level because the Internet is a decentralized system.

According to Sir Tim Berners-Lee, to create a "real kill-switch-off-device," governments should convert the Internet from a decentralized into a centralized system that they could control at their discretion (Prigg, 2013). In similar terms, the technical and academic sector agree on the fact that the key for the Internet to survive extreme situations is its decentralized system, which is not uniform all over the world (Bowman & Camp, 2013).

> "The internet by definition is a mesh of networks, so, like a leaky sieve, the bigger the mesh the harder it is to isolate all the connections." (Winder, para.4, 2011)

A decentralized system is not a characteristic for each nation-state; some nation-states have their Internet service distributed among multiple private companies that sometimes even have international partners (U.S., U.K., Germany f/e). Differently, in other nation-states, the service is provided mostly by a government-owned-company (Cuba, Venezuela, f/e). For governments in the second group (when a government-owned-company provides the Internet service), it is a lot

easier to act over the Internet infrastructure and deprive of Internet access to their population (Dyn, 2012).

In any case, the Internet architecture was built to be as interchangeable and resilient as possible. In consequence, Internet users can exchange information in different host nation-states and circumvent an Internet shutdown. The quality of the Internet service may be affected but getting Internet connection would be possible.

Here is where the answer to the question of feasibility faces a breaking point: although the 100% level of success shutting down the Internet may not be possible, depending on the circumstances of the infrastructure in each nation-state, the level of success may be very close to 100%. It is not the same to attempt to shut down the Internet in Eritrea or Somalia, (where there is a feeble, almost inexistent, Internet infrastructure) than to do it in a nation-state with a massive communication infrastructure, such as the U.S. Therefore, the answer to the feasibility question depends on the specific case.

While it may be easy to think that to shut down the Internet some governments would be willing to shut off all the borders at the top level ISPs, they just won't do that because they still need to be connected to international financial systems and their armies need access to their national systems (Subramanian, 2011).

1.3.4. Differences Between and 'Internet Kill Switch' and Censorship

An Internet shutdown, as described by this document and the academic literature is the attempt to stop all Internet activity within the borders of the territory of a nation-state (Opderbeck, 2012, 2013). It is considered the most extreme form of control over the Internet infrastructure

because government's' actions purpose is to stop all Internet activity in a nation-state. However, there are more usual and ordinary, less severe, forms of affecting the Internet, such as censorship. The next paragraphs will include a short explanation of the differences between censorship and an Internet shutdown. To explain these differences, I will define censorship and its types according the OpenNet Initiative (ONI), a research project at the University of Toronto. This is one of the most complex and reliable projects monitoring activities over the Internet infrastructure at a worldwide level.

Censorship is one of the forms through which governments limit access to specific sources of Internet content, rather than to stop all Internet activity and services that support Internet access. The most common types of censorship are the following ones (ONI, 2014):

1. Technical Blocking: there are three commonly used techniques to block access to Internet sites: Internet Protocol (IP) blocking, Domain Name Server (DNS) tampering, and URL blocking. These techniques prevent access to specific web pages, domains, or IP addresses. Authorities use these methods when they don't have jurisdiction or control over the websites they are interested in blocking. This scenario is the most common case of censorship against social media (f/e Twitter, Facebook, WhatsApp, and YouTube).
2. Search Result Removals: this occurs when private companies that provide Internet search services cooperate with governments to omit websites from search results upon the request of those governments
3. Take Down: this situation occurs when regulators have legal jurisdiction over web content hosts. The regulator only must demand the removal of the websites that according to its criteria are inappropriate or illegal content.

None of these censoring techniques is equivalent to what this dissertation defines as an Internet shutdown. Targets of these types of technique are very specific, whether is a web page, an IP address, a search result among others, but not the entire Internet. I will elaborate more on this matter in the next paragraphs.

The Internet Society (ISOC) alongside with other actors of the civil society[7] includes within the term "Internet shutdown" episodes of censorship and attempts to stop all Internet activity. ISOC defines Internet shutdowns from two perspectives:

1. "A total shutdown or blackout where all services on the Internet are blocked off, targeting mobile Internet access and/or fixed lines, such that users in a country or region are not able to access the Internet
2. A partial shutdown, where content blocking techniques are applied to restrict access to websites or applications, very often to block people from communicating or sharing information amongst them" (ISOC, 2017b, para.5)

In this regard, the definition of this dissertation, about what an Internet shutdown is, agrees with the first approach of ISOC, named "a total shutdown," but does not agree with the second one named "a partial shutdown". In my opinion, a partial shutdown that targets specific websites or applications is a case of censorship and not an Internet shutdown. As I will explain later in this document, most legal documents of the debate in the U.S. between 2009 and 2011, the episodes in Nepal, Myanmar and during the Arab Spring, refer to the term "Internet shutdown" as the government attempt to stop all Internet activity and not to target specific applications.

In my opinion, the distinction between both terms is not only necessary for academic purposes, when clear conceptual definitions are required. The distinction is also critical

[7]The referred project is known as #KeepItOn and is run by accessnow, a civil society organization: https://www.accessnow.org/keepiton/

because when policy makers, academics and other stakeholder discuss these forms of control over the Internet, their acceptance most likely will be different when facing an Internet shutdown than when they face a censorship. It is also important to say that, just like in the academic environment, clear definitions are required to create legislation and potential exceptions included in the law.

I will explain later in this document how advocacy groups and non-governmental organizations use all the terms previously described indistinctively or as synonyms of an Internet shutdown (accessnow, 2017; West, 2016).

1.3.5. DNS Poisoning

Although the TCP/IP model has five layers, average Internet users constantly interact only with the application layer, which allows writing postings in social networks, uploading pictures and performing primary activities on the Internet. Nevertheless, the application layer is only one, the highest one in the model[8].

The remaining three layers go down to the wires and cables that allow the communication, by addressing (identifying devices), routing (moving the information from one point to another) and naming (giving human-readable names to the IP addresses, also known as DNS) (Dyn, 2014c, 2014b).

Governments assume that if they "remove" one layer, everything below falls apart. Following this logic, governments believe that if they poison the DNS or remove it, the application layer will fail, and in that way, the Internet will be shut down. In this regard, DNS cache poisoning,

[8] This is the reason why some techniques call it the "penthouse suite" of the TCP/IP protocol.

also known as DNS spoofing, is an attack that exploits vulnerabilities in the DNS to redirect the Internet traffic away from legitimate servers towards fake ones. If an attacker gets control of a DNS server and changes some of the information on it, that DNS server would tell its users to look for something.com at the wrong address (Hoffman, 2016).

If various ISPs get their DNS information from the compromised server, the poisoned DNS entry will spread to the ISPs and be cached there. Then, it will spread to home routers (Hoffman, 2016; Mitchell, 2017). In 2010, a DNS poisoning event resulted in the Great Firewall of China temporarily going through China's national borders. This event ended censoring the Internet in the USA until the problem got fixed (Hoffman, 2016; Mitchell, 2017).

Poisoning the DNS slows down or prevents the access to web pages and services. Most likely mail, remote file systems and network printing may be inaccessible; everything that implies an external communication is at risk when the DNS does not work correctly (Lehtinen, Russell, & Gangemi Sr., 2012).

Another example of DNS poisoning affecting DNS resolvers like those of Google occurred during the anti-government protests from March 2014 in Turkey. Under normal circumstances, such queries would go to servers out of Turkish territory, which is how Turkish Internet users could circumvent the ban on YouTube imposed at the time. As a result of the DNS poisoning, local users of these DNS services were redirected to alternate providers controlled by Turk Telekom, the Turkish regulator (Zmijewski, 2014). In other words, Internet users believed that they were accessing Google's webpage for Turkey, but they were redirected to a space created by the Turkish government. When Google realized this situation, they made available the company's public address, so that people would type the IP address number instead of the webpage name

"google.com.tr". In this way, Internet users would have access to the real Google's webpage (Carstensen, 2014; Zmijewski, 2014).

A more recent example of DNS poisoning occurred in Venezuela in January 2019. Mr. Juan Guaido, President of the National Assembly, proclaimed himself as the interim President of Venezuela. This crisis catapulted a wave of Internet censorship activities such as blocking and filtering. While thousands of volunteers move to help with the distribution of humanitarian help that other nation-states sent to Venezuela, the Venezuela government started a phishing campaign driven by the major ISP owned by the government, CANTV. On February 12 all outgoing DNS traffic in and out of the IP address associated with voluntariosxvenezuela.com was returned with the IP address of a malicious site,159.65.65.194, which does not match the real site of the organization. The IP address of the malicious site is also returned by the DNS servers of CANTV (Azpura, Guerra, & Rivas, 2019)

1.3.6. The Internet: Decentralized System and Diversity in the ISPs

Because the decentralized Internet system is not uniform across the world, for some governments making a phone call and turning off power in a few central facilities is enough to disconnect the domestic Internet from the global Internet. This type of infrastructure also makes it harder for the government to defend the nation state's Internet infrastructure against an opponent who knows that targeting a few strategic points is enough. Facing this context, during the last ten years most nation-states have intended to achieve more diversity in their Internet infrastructure (Dyn, 2012; Ward, 2014).

In this regard, a study elaborated by Dyn (2012) explained the feasibility of shutting down the Internet according to the number of ISPs with international connections. ISPs with multiple international connections are the ones that purchased connectivity from another ISP outside of the nation-state territory where those ISPs are located. When more ISPs have access to global connectivity it is more difficult for a government to shut down the Internet (see table 01).

Table 01.- International Connectivity and Risk of Internet Disconnection

Nation-States with	Level of Potential Disconnection
ISPs with one or two International Connections	Severe risk of Internet disconnection
ISPs with fewer than ten International Connections	Significant risk of Internet disconnection
ISPs with at least ten internationally-connected service providers, but no more than 40	Risk of disconnection fairly low
ISPs with over 40 internationally-connected service providers	Extremely resistant to Internet disconnection

1.3.7. Rigorous Control

The more control a government exercises over the Internet infrastructure, the more difficult it is to circumvent the restrictions over the layers of the TCP/IP protocol. The level of success controlling the Internet infrastructure is the reason why some governments may be closer to achieve a full Internet shut down than other ones. A centralized system is the most convenient for regimes that wish to keep an active control over the Internet infrastructure, but many governments moved towards a decentralized system to protect their economic growth and market forces.

In successful decentralization cases, the government regulator facilitates the formation of several direct connections to international providers. If the regulator does not provide adequate

legal guidance, the diversification process will be slow in small markets, and the national incumbent provider (usually the traditional government telephone company) remains strong (Dyn, 2012; Ward, 2014).

1.3.8. Actors Involved: Some Facts

When in January 2011 Egypt digitally vanished from the international Internet traffic, this was the first time the entire world became aware of an Internet shutdown. However, shutting down the Internet is a practice dated back to 2005 and 2007, when the first episodes occurred in Nepal and Myanmar (former Burma) (K. Jones, 2005; OpenNet, 2006; Thompson, 2012).

Since then, different dictatorial and non-dictatorial regimes have tried to shut down the Internet. The empirical evidence suggests there are four different potential scenarios for Internet shutdowns:

1. Governments shut down the Internet within their territory.

   The first examples of this situation occurred, as mentioned previously, in Nepal and Myanmar in 2005 and 2007 respectively, and during the Arab Spring between 2010 and 2011 (in Egypt, Libya, and Syria) (Dunn, 2011; Streitfeld, 2013; Thompson, 2012). Similar cases occurred more recently in 2016 in Iraq, Bahrain, Ethiopia, Gabon and Cameroon (Billington, 2016; Karanja, Xynou, & Filasto, 2016; Ogundeji, 2017; Toor, 2016; Waddell, 2016a). This practice continues until 2018.

2. Governments shut down the Internet in other territories, as a cyberwarfare weapon.

The concept of cyberwarfare has been defined as the group of actions taken by a nation-state or international organization to attack and attempt to damage another nation-state's computers or information networks (RAND, 2017).

One alleged case of an Internet shutdown as a cyberwarfare weapon involved North Korea in 2014. On November 24, 2014, a hacker group "Guardians of Peace" (GOP) leaked confidential data from the Sony Pictures. The GOP used a variant of the Shamoon wiper malware to erase Sony's computer infrastructure and demanded that Sony withdraw its film "The Interview," a comedy about a plot to assassinate North Korean leader Kim Jong-un. Sony canceled the film's formal premiere and the U.S. government and intelligence officials claimed that the attack was sponsored by North Korea. However, North Korea denied any responsibility (Peterson, 2014).

On December 22, 2014, the Internet in North Korea went down after being unstable for two days. At the time, North Korea had 1,024 official Internet protocol addresses approximately and had only one government owned ISP, Star Joint Ventures. This ISP depends on China Unicom, China's government-owned telecommunications company. The North Korean Internet shutdown occurred just after President Obama claimed the U.S. would send a "proportional response" to what he called an act of "cybervandalism" against Sony Pictures. President Obama also blamed the North Korean government for the cyberattack Sony suffered. At the same time, the North Korean government blamed the U.S. for the Internet shutdown (Cheng & Nam, 2014).

U.S. officials described they were focused on the North Korea's telecommunications connections through China. They also claimed that they asked the Chinese government for

help in cutting off the North's ability to execute cyberattacks, but also denied to explain any further involvement (Cheng & Nam, 2014; Perlroth & Sanger, 2014).

3. Actors cut Internet fiber optic cables. There are at least two alleged cases of a ship cutting the Internet fiber optic cables. None of these cases offered evidence that cables were affected. However, it is important to mention that both episodes refer to the same ship: the Russian vessel Yantar (AIS Marine Traffic, 2017). Yantar was spotted in front of U.S. coasts in October 2015, and national security agencies manifested their concern of possible activities of this ship over the U.S. cables. The same ship was spotted in front of Syrian coasts in October 2016 and its presence occurred at the same time that an Internet shutdown occurred in that nation-state (Belson, 2016; CircleID, 2016; Sanger & Schmitt, 2015; Sullivan, 2016).
4. Actors considered "anonymous organizations," may have tried to shut down the Internet in the territory of a nation-state. A situation of this kind occurred in 2013 when the hackers group Anonymous threatened Israel that they would shut down the Internet in that nation-state if the government shuts down the Internet in Gaza (Moore, 2015; RT, 2013a). Had Anonymous being successful, this would be a concrete possibility of a non-governmental actor shutting down the Internet.

The empirical evidence also suggests that governments' attempts to shut down the Internet may be restricted only to a city, region or facility, instead of the entire territory of a nation-state. Examples of this capability occurred in: (1) the province of Xinjiang, China in 2009 (Economist, 2013; MacKinnon, 2012), (2) the city of San Cristobal in Venezuela in 2014 (Obrien, 2014), (3)

eleven states in India between 2015 and 2016 (CCG-NLU, 2016; Pahwa, 2015, 2016) and, (4) at to some extent the BART[9] San Francisco episode within U.S. territory. (BART, 2011; Bell, 2011).

1.3.9. National Security: The Arrangements between Governments and Geopolitics

As I previously mentioned, the main reason why governments interfere with Internet service is the existence of what they declare is a national security situation. This section will try to explain what national security means from a conceptual point of view to the life and survival of nation-states.

Nation-states, as entities, create a state with the purpose of providing benefit to the nation it governs; however, the goal of the state is also to guarantee the survival of the nation-state itself as the central entity of international law. Within this context, nation-states also created the concept of national security (Bobbitt, 2002). In this line, and following the tradition in political science research, national security refers to the safety of the territory and population of a nation-state and by extension to the policies adopted by its preservation (Paleri, 2008).

For some academics, national security is a "constructed concept" for any nation-state at any given time. Multiple factors, like political priorities and the media, will play a role securitizing specific issues known as "security priorities" (Richards, 2012). Security priorities, thinking in

[9] Bay Area Rapid Transit -BART- is rapid transit system serving San Francisco Bay Area. A government company, the San Francisco Bay Area Transit District is BART's operator. In August 2011, BART interrupted cell phone service on its platforms; according the company, they did this to prevent a possible protest. A month before, on July 3, 2011, a man was killed during a confrontation with transit police. The company interrupted the service in specific BART stations. Activists criticized BART's actions because they consider them as a violation of the First Amendment. During the BART episode, the DHS took responsibility for shutting down the mobile service during a protest in the transit system serving San Francisco Bay Area (BART, 2011; Bell, 2011).

global terms, change over time. Examples to be cited are periods like World War I, World War II, the interwar, the cold war and the period after. Securitized issues and the actors involved changed; new security actors and dimensions that moved beyond the traditional military sphere into civil, commercial and private aspects replaced them. To be more specific, it is important to mention that the concept of national security (in contraposition of the general concept of security) depends explicitly upon the priorities of each nation-state (Richards, 2012).

Because of such a broad definition and different priorities all over the world, many governments have justified their actions on the grounds of national security. This point is important because national security defines a particular concept, a specific set of security priorities and concerns determined by political leaders of a nation-state (Paleri, 2008). That set of priorities and concerns is known as the "national interest". The national interest will define the way nation-states act in particular circumstances (Richards, 2012).

Generally, in democracies, the definition of national interest and national priorities is subject to debate. Depending upon the specific circumstances, the definition of national security shall be the result of "permanent necessities of geopolitical position" or the requirements of external conflicts when the nation-state faces a war in the classical sense. In non-democratic regimes, the national interest is subject to the elite and the political leader of the government (Bobbitt, 2002; Richards, 2012).

1.4. Governments' Regimes Classification

One of the core elements of this project is the idea that shutting down the Internet is a governmental action (or at least there is some level of government involvement) that involves not

only authoritarian but also democratic and hybrid regimes. This section clarifies the differences between these concepts.

Traditional classifications established a dichotomy between authoritarian and non-authoritarian regimes, and the fundamental distinction has been the way how their rulers achieve power (Morlino, 2008, 2009). Democratic governments are supposed to gain power through national elections, and authoritarian regimes usually get to power through a coup d'état or another illegitimate mechanism. However, the traditional dichotomy has been replaced by new and different categories.

Government regimes are the conjunction of government institutions and rules that are "either formalized or are informally recognized as existing in a given territory and with respect to a given population" (Morlino, p.3, 2008). For this research, I will use the government regimes classification of the Economist Intelligence Unit (EIU) measure of democracy from the Economist group.

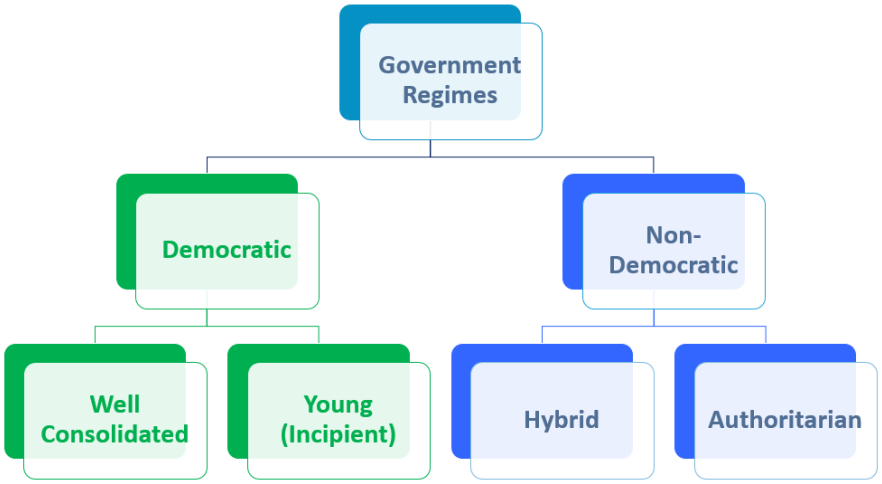
I chose this classification for two reasons:

1. It includes different variables to evaluate a regime, other than the traditional division based on the electoral vote.
2. The traditional dichotomy of considering only democratic and non-democratic regimes has been replaced by a classification that includes the possibility of varying degrees of democracy. This classification provides a wide range of scores, including developed and developing nation-states.

The EIU index of democracy is the result of the ratings for 60 indicators grouped in five categories: (1) electoral process and pluralism, (2) civil liberties, (3) the functioning of government, (4) political participation and (5) political culture. The result is built according to the

average of these categories (EIU, 2008). From the EIU perspective, nation-states belong to one out of four types of regime, such as "full democracies," "flawed democracies," "hybrid regimes" and "authoritarian regimes" (EIU, 2008). This research will use the same parameters as the EIU classification, but will use the terms "consolidated democracies," (instead of full democracies) "young democracies" (instead of flawed democracies) and "hybrid regimes" (Please see figure 04).

Figure 04.- Types of Government Regimes



This dissertation will focus in two types of non-authoritarian regimes, consolidated democracies and hybrid regimes. This classification follows specific factors related to the political context of the cases under study; therefore, this is a political classification. I preferred this classification over economic, geographical, technical or economic for the following reasons:

1. This dissertation starts from a presumption that I intent to challenge: that well consolidated democracies don't shut down the Internet and never consider doing so. This challenge started as a motivation after reviewing that most of the academic literature studied Internet shutdowns as an effective way to control the flow of

information in authoritarian regimes. This is the reason why I selected consolidated democracies as case studies. Hybrid regimes were the next complementary group, as these are not considered authoritarian regimes either.

2. The political assumption that shutting down the Internet was an extreme policy executed only for authoritarian regimes has no parallel in economic or technical terms. This means that there are no studies or assumptions that conclude that developing nation-states have tendency to shut down the Internet and that developed nation-states do not. Same reasoning applies to nation-states with a least developed Internet infrastructure.
3. In geographical terms, Internet shutdowns are worldwide spread. Whether they effectively occurred or political administrations conducted a debate on the subject, I found them all over the world. It is important to clarify that the American continent remains as the one with the least number of debates on the subject and with only one episode on the subject. This is the reason why at least two of the cases I selected belong to the Americas.

1.4.1. Consolidated Democracies

The definition of what a democracy is and how to measure is an ongoing debate. The concept itself has a long history; something similar to what today is known as democracy, existed in classical Greece, but the concept is not the same (Carpizo, 2007).

According to some academics, a consolidated democratic regime shall be characterized by: (1) a government based on majority rule, (2) the consent of the governed, (3) the existence of free

and fair elections, (4) the protection of minorities, (5) respect for basic human rights, (6) equality before the law, (7) due process of law and (8) political pluralism (Morlino, 2008).

Therefore, a definition of democracy should at least include the following characteristics: (1) universal suffrage independently of gender, (2) free, competitive, recurrent and fair elections, (3) more than one party, as an expression of political pluralism and (4) different and alternative media sources (Dahl, 2005; Morlino, 2008).

Free elections and clean electoral processes, alongside with respect to civil liberties or constitutional rights, are required and basic conditions to achieve democratic regimes. However, they are not enough to have a consolidated democracy (EIU, 2007). “Alternation” in power is also necessary because it creates a presumption about democracy, although, that is not a necessary pre-condition (Sartori, p.p.199-200, 1974, as cited by Linz, 2000).

According to the EIU criteria, the first steps to identify a regime as democratic or not are the following critical areas: (1) whether national elections are free and fair, (2) the security of voters, (3) the influence of foreign powers on government, (4) the capability of the civil service to implement policies and, (5) the presence of different media sources belonging to different proprietors. Although a perfect democracy is unlikely to exist, any regime that fulfills the previous critical areas may be considered a consolidated democracy. If one of these requirements is not met, or at some point ceases to be so, the regime in question is no longer a consolidated democracy (EIU, 2007).

1.4.2. Young Democracies

Young democracies do not fulfill one or more of the requirements to be a consolidated one. Their main characteristics are (EIU, 2008): (1) deficient levels of political participation, (2) weak democratic cultures and (3) backsliding in media freedoms.

Young democracies have free and fair elections, but empirical evidence shows that even though these regimes face political problems, like infringements on media freedom, fundamental civil liberties or constitutional rights are usually respected. At the same time, these regimes face significant weaknesses in other aspects of democracy, mainly governance problems (most likely week institutions), underdeveloped political culture and low levels of political participation (EIU, 2011).

1.4.3. Hybrid Regimes

Hybrid regimes are also known as “transitional regimes” or “trapped regimes” because they are between a non-democratic set of practices (like traditional, authoritarian and post-totalitarian regimes) and a democratic one (mainly a young democracy). Therefore, hybrid regimes are those that have in parallel some of the representative institutions and procedures of democratic systems and some authoritarian or traditional features (Morlino, 2008). Hybrid regimes resemble democratic ones, mainly because they celebrate multi-party elections, but lack other characteristics of democracy. Hybrid regimes don’t oversee a peaceful transition of power between parties through the electoral defeat of the incumbent, and lack of free press and insurance for political and civil rights (Alexander, 2008).

In the specific case of hybrid regimes, there are three possible hypotheses for their existence (Morlino, 2008): (1) the regime is borne out of an authoritarian regime, (2) the regime is borne out of a decolonization process from a traditional regime, such as a monarchy and (3) the regime is borne from the crisis of a previous democracy (usually a young one). Most cases in the last decades belong to the first category, nation-states in transit from an authoritarian regime. The main characteristics of hybrid regimes are (EIU, 2007; Morlino, 2008):

1. Groups of the opposition are formally allowed to participate in the political process, but have little possibility of governing,
2. There is one hegemonic and dominant party, inside of which there may be competition among the leading candidates,
3. Although there is some degree of real participation, it is usually minimal and limited to the election period, with the possibility of having contested elections and fraud allegations
4. There is little institutionalization in the army forces, and they maintain an evident political role, although it is not explicit and direct.

1.4.4. Authoritarian Regimes

Authoritarian regimes are those in which the ruling authority keeps itself in the highest political position, mainly because of "a combination of appeals to traditional legitimacy, patron-client ties, and repression" (Linz, 1975, p.252 as cited by Inkeles, 1991). An apparatus of personal loyalties close to the ruling authority carries all of it. Authoritarian regimes have been the norm for much of the human history at least until the 1970s. Until 2010, about one-third of the world's nation-states were considered authoritarian regimes (Frantz, 2011; Inkeles, 1991).

In the beginning, during the “foundational moments” of the authoritarian regime, the way decisions shall be made remains as an uncertain and unclear process, even for direct participants. Although there is usually a citizen coalition supporting the seizure of power, only a few of those citizens will be able to influence government decisions (Geddes, 2004).

Another characteristic of authoritarian regimes is that they impose de-facto-limits on minorities’ freedoms and also establish a legal framework for those limits, assigning the interpretation of that legal framework to the rulers themselves, instead of to independent and objective legal bodies (Linz, 2000). In the political realm, politics is in a constant interplay between two actors: elite and political leader(s). These actors are in continuous conflict, elites compete against a dictator and also against each other; while the antagonism prevails, authoritarian institutions frame the rules or dynamics of this struggle (Frantz, 2011).

Professionalized military or a political party are usually the ones that govern an authoritarian regime (Linz, 2000). When the regime becomes stronger and more confident, there is an increase in government control and repression of any independent media and increasing attacks on independent journalists (EIU, 2007). Government control and repression of any independent press is a characteristic of an authoritarian regime, and it tends to become worse, mostly attacking independent journalists (EIU, 2008).

2. Literature Review and Theoretical Framework

This chapter provides a review of relevant legal analysis and social science literature related to government control over telecommunications, such as the Internet, and it is composed of four parts. First, it examines the conflict between nation states' traditional jurisdiction concept and the Internet open architecture design. Second, this chapter addresses the complicated situation of the governmental control over the Internet infrastructure in authoritarian and democratic regimes. I will take as examples the Arab spring and administrative control over the telecommunications in the U.S. When providing a technical overview, I will mention some of the concepts introduced in the first chapter. The third part of this chapter presents an overview of the gaps in the current literature, which offered opportunities for an exploratory study about the process of shutting down of the Internet, as a form of government control. Finally, the last part of this chapter presents an overview of President's power to execute the laws, known as the unitary executive theory, and the chosen theoretical framework for the proposed study, the securitization theory of the Copenhagen school.

2.1. The Internet and the Nation-States' Traditional Boundaries

This chapter will address the conflict between the classic nation-states' sovereignty model, territorially based, and the Internet, a technology that does not recognize traditional territorial borders or any governmental authority (Mueller, 2010; Rosenne & Hague Academy of International Law, 2004).

For most part of the twentieth century, nation-states have been the primary source of (1) law, (2) policies and regulations and (3) constructions of national security (Bobbitt, 2002; Slapper & Kelly, 2008). In such condition, and because their governments can execute their laws within their territorial boundaries, nation-states have created different regulations over the Internet infrastructure located within their sovereignty. This characteristic makes nation-states powerful actors when talking about Internet regulation. This chapter will define why nation-states are considered the primary entities in the international realm and why the Internet challenges one of their more essential elements, their sovereignty.

Legally speaking, and in according to the classic legal literature, nation-states are considered the main subjects of international law. They are entities that possess international rights and obligations, a condition known as "international personality." Nation-states, in particular, have the following capacities (Brownlie, 2003):

1. Maintain its powers by making international claims
2. Negotiate and sign treaties and agreements valid at an international level
3. Enjoy privileges and immunities from national jurisdiction

The last capacity of nation-states, the enjoyment of national jurisdiction, is subordinated to the existence of territorial borders, as nation-states only can exercise jurisdiction within the boundaries of their territory (Kulesza, 2012).

Additionally, according to the declarative theory of statehood, every nation-state must have the following qualifications, also known as "statehood elements" (J. Crawford, 2013):

1. Population: a stable community of people;

2. Territory: physical basis for the existence of a state; a reasonably stable political community must be in control of a certain physical area (a strictly defined frontier is not required). A state's territory also includes its appurtenances, airspaces and territorial sea;
3. A Government: a legal order for a political community established in a certain area; and
4. Independence: capacity to establish relations with other nation-states

The legal competence of nation-states depends on the existence of a stable delimited homeland (Benadava, 1982). The main elements of legal competence are sovereignty and jurisdiction (Brownlie, 2003). In this way, the general principle of the international law reads that nation-states are entities with the capacity to exercise jurisdiction through the actions of their governments over the population within the borders of their territory (Brownlie, 2003; J. Crawford, 2013). In this way, jurisdiction is the capacity to apply the national legislation within nation-states' boundaries without the interference of foreign power (Benadava, 1982).

The Internet is a challenge to the traditional concept of one nation-state jurisdiction because it may present a criminal case with multiple domains involved: a victim, a criminal and the material qualified as *"corpus delicti,"* all of them could be in different territories. In this example, there is a problem with a "triple" jurisdiction, which is the rule (and not the exception) when criminal activity on the Internet is involved (Rosenne & Hague Academy of International Law, 2004).

Attached to the concept of jurisdiction is the idea of government control within some specific territorial borders. Therefore, the Internet challenges both, the conventional concept of the nation-state and the Westphalian model of sovereignty. This controversial characteristic of the Internet is the reason why many legal scholars consider the Internet a "perplexity" of the modern international law (Kulesza, 2012; Rosenne & Hague Academy of International Law, 2004).

From a social sciences perspective, nation-states are defined as strong institutions and the leading suppliers of public governance (Mueller, 2010). Nation-states' main strength is the exercise of their control (their coercive capacity) by creating institutions, rules, and regulations based on the traditional claim of guaranteeing their survival. As it was in past centuries, nation-states still make decisions according to their interests and the position of power they have in the international community (Bobbitt, 2002; Khan, 2007). Their way to act in the international realm reflects a strategic approach usually based on the use of force as the chief arbiter of foreign affairs (Bobbitt, 2002).

This realist approach from international relations established after World War II enabled transnational corporations to increase their activities beyond the borders of nation-states' territories. However, nation-states did not disappear, and they changed to survive and reasserted their strength following three steps (Braman, 2006):

1. Nation-states learned to use the same type of "informational power" that private corporations and other non-state actors used to challenge the strengths of different geopolitical entities.
2. Nation-states developed techniques to extend the participation of private sector entities as regulatory agents, "turning private centers of power to state purposes" (Braman, 2006, p.34). A widespread example is the involvement of Internet service providers (ISPs) in helping governments to monitor the Internet for security purposes and intellectual property rights abuses.
3. Nation-states main characteristic is that they are "networked" because of the way they relate to other nation-states and non-state actors. By changing according to the demands of

the new century, nation-states remain as the primary dominant political actors in the international community (Bobbitt, 2002; Braman, 2006).

It is important to point out that, despite the nation-state's predominant role, they must share the international realm with non-state entities. In 1949, the International Court of Justice (ICJ)[10], the international court that solves issues when multiple jurisdictions are involved, opened the door for new interpretations about what international legal personality means.

After the assassination of a Swedish diplomat, the Count Folke Bernadotte, the ICJ established in an advisory opinion that the United Nations (UN) had "international personality" as a nation-state would have. Therefore, the ICJ then acknowledged the existence of other actors with the capacity to act in the international realm, besides the classic nation-states.

The central question the ICJ analyzed was whether the "capacity to bring an international claim" is an attribute only from nation-states, or also an attribute of international organizations. The court stressed that although the UN international legal personality is not identical to that of a nation-state, the organization was "capable of possessing international rights and duties" and had "capacity to maintain its rights by bringing international claims" (ICJ, 1949, p.1).

Today, besides nation-states, the ICJ recognizes as subjects of international law non-state actors such as individuals, international organizations, multinational companies, international non-governmental organizations, cover states, entities legally proximate to states, entities recognized as belligerents and international administration of territories before independence (Brownlie, 2012).

[10] The International Court of Justice is the main judicial organ of the UN. It was created in 1945 by the UN Charter and began working in April 1946 (ICJ, 2017). It is also known as the World Court and is based in the Peace Palace in The Hague, Netherlands. The main function of the Court is to solve disputes among nation-states, and to provide authoritative and influential advisory opinions on issues referred by international organizations, agencies and the General Assembly (Kolb, 2013).

Forty years later, since the early 1990s, the dominant view in the international realm was the transformation of the world through non-state actors, a process known as "globalization." New technologies, in particular, a non-territorial new medium, like the Internet, were supposed to supersede nation-states' old institutions and create new and more efficient ones. However, these hopes may have underestimated the nation-states' role and its institutions, and the difficulty of replacing them. The current world financial and migratory crisis discredited the position of the market and called again for the restoration of the nation-state power (Grygiel, 2016; Mazower, 2014).

2.1.1. The Internet: A Challenge to the Nation-States' Sovereignty

Jurisdiction is the exercise of sovereignty, and government control exists because governments are sovereign within their territorial borders. As established previously, governments, as administrative entities of nation-states, enforce laws and regulations within the limits of their territory (Braman, 2010; Kulesza, 2012). Therefore, to be a nation-state, independence is required from any external authority or force to administer the law; this is the most basic definition of the classic sovereignty (Kulesza, 2012).

The Internet represents a problem for government sovereignty and jurisdiction because the Internet is global and activities within the Internet domain involve multiple jurisdictions, and therefore many sovereignties and many nation-states. In this sense, the Internet challenges governments' traditional authority to regulate social and international relations based on territory and the conventional concept of sovereignty (Braman, 2010; Kulesza, 2012; Rosenne & Hague Academy of International Law, 2004).

This conflict between Internet and nation-states is based on the fact that nation-states' sovereignty is "territorially bounded" and the space created between networked computers is a non-territorial space (Mueller, 2010). Facing this situation, the idea of controlling the Internet represents a new challenge for governments all over the world, whether they are democratic or non-democratic regimes.

We can find an example of this jurisdictional and sovereignty problem when the Internet is involved in the "Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France (LICRA c. Yahoo!)," known as the Yahoo case. The Yahoo case is initiated by a French citizen, Marc Knobel, fighting against neo-Nazi propaganda he discovered on a Yahoo!'s auction website. The propaganda violated French law which banned the trafficking of Nazi goods in France. Mr. Knobel argued that that France had the right to defend itself from any illegal sale from the U.S. and, his lawyers demanded Yahoo about why that company should be exempt from French law (Goldsmith & Wu, 2006).

Yahoo's defense was that the French website, www.yahoo.fr could complied with French law, but the U.S. website, which did not have to complied with French law and could still be visited by French citizens. Since Yahoo could not identify the location of the users accessing the Nazi propaganda, compliance with French law would require removal of all Nazi items from the U.S. website. Yahoo refused to accept French law as "the effective rule for the world" (Goldsmith & Wu, 2006, p.5).

The French court ruled against Yahoo and ordered the company to take all provisions to make impossible visits by French web surfers to the illegal Yahoo sites. Yahoo contested the jurisdiction of the French court, but the court rejected this petition claiming jurisdiction on the theory that Yahoo's conduct caused harm in France (Goldsmith & Wu, 2006).

On the other hand, Yahoo started proceedings in a U.S. court and the outcome was a ruling in favor of the company. The ruling of the U.S. court adopted the position of the company that the French law was not applicable to a company with headquarters in the U.S. and that imposing geolocation components to identify the whereabouts of those who want to access the Yahoo website was a first amendment violation. From the U.S. perspective, the First Amendment protects a broad spectrum of hate speech, while there is a different set of limits applies to the speech in other nation-states, including France. This difference was what created the dispute in the *LICRA v. Yahoo!* case (Greenber, 2003).

Then the contentious issues here are: "(1) whether Yahoo may be prosecuted in France under French law for maintaining both auction sites that sell Nazi-related items and information sites promoting Nazi doctrine and (2) whether U.S. courts should enforce the resulting judgment" (Greenber, 2003, p.1191).

Although at the beginning Yahoo didn't comply with the French ruling, after warnings from the French court that it would issue fines up to $13,000 a day, Yahoo agreed to take down all Nazi memorabilia from its various auction sites (Goldsmith & Wu, 2006).

As mentioned before, the Internet is not supposed to recognize territorial borders because of its open design. One of the challenges of the Internet is how to solve a problem by applying existing legal principals to the digital world or if new legal doctrine is required. Nevertheless, governments (on behalf of their nation-states) defined as very important sources of public governance keep imposing (or at least trying to) their jurisdiction and therefore they try to extend their sovereignty (Mueller, 2010).

Although the builders of the Internet tried to create a "root system" that would allow them to create a sort of "independent territory" of the governments by using "domain names" and

"Internet Address), this tactic has not been clearly successful as governments interfere and try to take control over the root zone (Goldsmith & Wu, 2006).

The Yahoo case was a success from the point of view of the nation-states where they use their coercive capacity to execute its local legislation. This matter was one of the earliest cases that put on the table the issue of why the Internet is called a "perplexity" for the international law where traditional mechanisms to solve a controversy are not applicable.

Up to today the question of whether litigation in multiple courts all over the world is the best way to resolve the Internet international disputes remains a controversy. In any case national governments try to take control of the Internet by using any coercion capacity within the borders of their territory, before trying to take any measure in the outside borders.

2.1.2. The Complexity of the Internet

The Internet has been considered one of the new communication media that governments cannot control. Facing this circumstance, the concept of the Internet has evolved to be more than just a communication technology tool. The term to explain this condition is "complexity" (Giacomello, 2005) and in the next paragraphs, I will describe what it means.

Complexity is one of the essential characteristics of the Internet. The Internet's architectural design, implemented by packet switching, is well known for its efficiency, flexibility, resilience, and lack of a single node or centralized control (Horvitz, 2013). The complexity lays in the fact that the Internet is formed by networks that decide when and how to interconnect with each other without any additional control (Faratin et al., 2007). According to the academic literature, the complexity of the Internet is the result of three factors:

1. The Internet is an "infrastructure" (an actual computer network) that allows the functioning of other distribution networks, like water, gas, energy, and economics. (Clavio, 2008; Giacomello, 2005).
2. The "multiple jurisdictions" of the Internet. There are national and international authorities, but there is no entitled or competent authority to regulate, monitor and maintain the Internet (Braman, 2006).
3. The multiplicity of stakeholders involved, such as national governments, the private sector, and non-governmental organizations. All individual actors from the three groups at some point may form an alliance to increase or to resist control over the Internet (Nye & Donahue, 2000).

From a technical point of view, the complexity of the Internet implies that there is no central node (as a connection point) and therefore, its management structure is limited to a few internal functions. The lack of a centralized structure allowed the Internet "to be responsive to a very large unregulated constituency and allowing explosive growth and with increasing usefulness to its users" (Horvitz, p.6, 2013).

Facing the possibility of losing control over the telecommunications within their territories, governments provide different reasons about why they are (or would be) compelled to act on the Internet information flow. According to the academic literature and political news, this study has identified the following reasons as the most common:

1. To protect the critical infrastructure, a vital element for the survival of nation-states, and therefore, an integral part of the national security policy (Homeland Security & Governmental Affairs Committee, 2010; Radvanovsky & McDougall, 2009),

2. To keep social control, which is vital for all types of regimes, because of the potential impact over civil liberties (Arnaudo, Alva, Wood, & Whittington, 2013; Bowman & Camp, 2013; Dunn, 2011; Giacomello, 2005),
3. To perform an "upgrade" over the Internet infrastructure. In Algeria in 2015, the new Minister of Information and Communication technology pointed out that the main ISP had to implement a better infrastructure to conduct a "digital transition" (Farid, 2015),
4. To avoid school students cheating on their examinations. Although this explanation may seem absurd, this is what happened in Iraq in May in 2015 and 2016. May is the time of placement exams for sixth-year-school-kids and, as human rights groups were informed, the government ordered Iraqi telecom companies to slow down the Internet service and later on, to shut down it down to prevent cheating (Waddell, 2016a, 2016b). Syria and Ethiopia used a similar justification between May and June 2017. Syria even schedules more than one shutdown for this purpose (Dyn, 2017; Ismail, 2017; IT News Africa, 2017; Latif Dahir, 2017).

Different regimes, democratic or non-democratic, address the problem of the complexity of the Internet and the government control over the Internet infrastructure differently (Barnard-Wills & Ashenden, 2012). However, in general, national security is the most symbolic act of governments' authority, because each government decides what national security is for its own nation-state (Paleri, 2008; Richards, 2012). Two perspectives of this problem, for non-democratic and democratic regimes, alongside with the international standards established by CCPR will be explained next.

2.1.3. International Covenant for Civil and Political Rights (ICCPR)

ICCPR is a multilateral agreement that represents a worldwide effort to achieve consensus in the treatment of civil and political rights. This international agreement was adopted by the UN in 1966 and opened for signature the same year. ICCPR got in force on March 23, 1976, and currently, 168 nation-states have ratified the treaty (UNTC, 2016). The primary purpose of ICCPR is the protection of fundamental rights like political participation, due process, non-discrimination, freedom of expression, assembly and religious freedom in particular (Cole, 2011). To achieve this goal, ICCPR requires nation-state members to make reports of their progress in working towards the achievement of the rights contained in the treaty (Keith, 1999).

Like other human rights agreements, ICCPR regulates how governments behave towards their citizens, instead of regulating the behavior among nation-states, which is a constant characteristic from other international treaties. ICCPR represents a final negotiation among almost all nation-states of the world, and it covers, to the extent possible, all views about civil and political rights of the nation-states that subscribed and ratified the treaty (Cole, 2011; Keith, 1999).

As any other treaty, ICCPR cannot be imposed to a nation-state; as sovereign entities of international law, nation-states decide if they will submit their local jurisdiction or not to the international order. The execution of ICCPR is subordinated to the government behavior within the borders of its nation-state territory (Forrest Martin, Schnably, Wilson, Simon, & Tushnet, 2006; Mathiason, 2009). Nation-states that ratified ICCPR assume the obligation of ensuring the right of freedom of expression (Mathiason, 2009). Nevertheless, ICCPR also allows for situations when the power can be restricted, as stated in section 19 (3.2) of the treaty:

> "International Covenant for Civil and Political Rights (ICCPR).-"
>
> "Article 19."
>
> "1.Everyone shall have the right to hold opinions without interference."

> "2.Everyone shall have the right to freedom of expression [bold added]; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, orally, in writing or in print, in the form of art, or through any other media [bold added] of his choice."
> "3.The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions [bold added], but these shall only be such as are provided by law and are necessary:"
> "(a) For respect of the rights or reputations of others;"
> "(b) For the protection of national security or of public order (ordre public), or of public health or morals."

Regarding the pertaining to a "state of emergency" or a "national security threat," the ICJ and the European Court of Human Rights (ECHR) define a "state of emergency" as the consequence of a threat of war or a public emergency threatening the life of a nation-state (Andrew Murray, 2003; D. Murray, 2009). ICCPR does not include a definition of "national security," and there is not yet a definition for this concept in any other international agreement (Mathiason, 2009).

To explain the limitations to the right of freedom of expression, ECHR established that such restrictions must be subject to very particular and rigorous requirements. Those requirements include a test of necessity and proportionality to be "constructed strictly" and "established convincingly" (European Court of Human Rights, Surek and Ozdemir v. Thrkey, 23927/94 and 24277/94, para 46(i), as cited by D. Murray, 2009).

2.1.4. Non-Democratic Regimes

Authoritarian regimes claim that they must control the Internet to fight against cyber-attacks and terrorism, but also to protect their critical infrastructure. Nevertheless, for these

regimes controlling the Internet content is more important than managing the critical infrastructure (Gibbs, 2004).

Another characteristic of authoritarian regimes is that they coerce the private sector to participate according to their needs in their national security policies; they do not see the private sector as a partner but as a source of information (Boas, 2006; Giacomello, 2005).

2.1.4.1. Historical Context: The Arab Spring

On December 17, 2010, Mohamed Bouazizi, a young Tunisian street vendor, set himself on fire after trying to fight against an inspection fee. Bouazizi appealed to the police, then to municipal authorities and even to the region's governor. Following every appeal, security officials beat Mohamed (Howard & Hussain, 2013). After being humiliated constantly by the Tunisian security apparatus, Bouazizi set himself on fire and several days later died on January 4, 2011 (Abouzeid, 2011).

The state-run and traditional media did not cover Bouazizi's death, so people spread the word through blogs and text messages. In that way, many people sympathetic towards Bouazizi noticed that they shared similar problems. By the time Bouazizi died, national protests were spread all over Tunisian territory (Howard & Hussain, 2013).

Since 1995, the Tunisian government had interfered with digital networks for political reasons more than any other state, but after Bouazizi's death, the government tried to ban Facebook, Twitter, and video sites, but revolutionaries found their way around the ban. Ben Ali's regime (the Tunisian President) fell apart very quickly, and he abandoned Tunisia on January 14, 2011. In this way, traditional political structures in the Middle East and North Africa (region

known as the Arab world) were challenged, and revolts in Tunisia and Egypt encouraged young people across the region creating massive demonstrations in the streets (Asseburg, 2012; Howard & Hussain, 2013).

This uprising would be the beginning of what it is known as the "Arab Spring" (Abouzeid, 2011). After the Tunisian case, other nation-states of the Arab world would face national uprisings and demands for political changes, such as Egypt, Libya, Yemen, and Syria (currently embedded in a civil war) (Asseburg, 2012; Barnard & Mackey, 2012; Slim, 2016).

2.1.4.2. The Arab Spring: Two Points of View

The Arab Spring phenomenon attracted commentators who emphasized the role of social media, and therefore the Internet, to define the Arab Spring as a "social media revolution," by focusing on its organization aspects and information spread (Comunello, 2012). In this scenario, academics and non-academics credited the Internet with a crucial role in the political process of the Arab Spring (Auer, 2011). However, the academic literature is divided about this fact. The main reason for such division is that democratization movements existed long before the Arab Spring and certainly before mobile phones and Internet, which makes it difficult to conclude if their existence and use were the reason for the success of the Arab Spring in many nation-states (Howard & Hussain, 2013).

For those academics who consider the Internet as a catalyst for the events of the Arab Spring, to mobilize pro-democracy and lead a revolution, the Internet became a massive media tool for activists (Harlow & Johnson, 2011b; Lotan & Graeff, 2011).

On the other hand, others minimized the role of the digital technology claiming that only a minority of people had Internet access and that similar "revolutionary" processes in the Arab World happened before the Internet existed (Anderson, 2011). For these academics, the most important aspect of the Arab spring was not how activists used technology to share ideas and tactics, but how and why activists' ambitions and techniques influenced local contexts at the point of organizing a revolution. That influence took place in traditional settings, such homes, and mosques, and not in the social network platforms (Anderson, 2011; Tufekci & Wilson, 2012). They reminded us how very similar historical contexts had taken place before:

> "In Tunisia, protesters escalated calls for the restoration of the country's suspended constitution. Meanwhile, Egyptians rose in revolt as strikes across the country brought daily life to a halt and toppled the government. In Libya, provincial leaders worked feverishly to strengthen their newly independent republic.
> It was 1919" (Anderson, p.1, 2011)

According to Harlow & Johnson (2011), during the Arab Spring, coverage in traditional media did not explain the core problem that generated the massive nationwide protests. On the contrary, general press in Egypt and Tunisia focused more on the drama and violence of the protests. Complaints of the protesters regarding Egyptian leader Hosni Mubarak's thirty-year-administration were minimized to one or two sentences and were presented as part of the spectacle (Harlow & Johnson, 2011a, 2011b; Howard & Hussain, 2013).

When the Egyptian government shut down the Internet on January 25, 2011, Egyptian citizens and hackers all over the world worked together to restore the Internet access. The interruption of Internet service had the opposite effect of what the Egyptian government expected. Far from generating isolation and separation, more people came together in Tahrir Square to protest for democratic changes. Protesters included Internet connectivity as one of their more critical demands (Andrews, 2012; Thompson, 2012), and they found creative ways to bring the

Internet service back using fax machines, old dial-up modems, and landlines to call Internet service providers in neighbor states for the cost of a long distance phone call (Andrews, 2012; McDowell, 2011).

Egyptian protesters located themselves close to the Egyptian land borders, and there they were able to use cell phone service from the nearest nation-states (e.g., Israel) (Andrews, 2012). When the Internet service in Egypt was interrupted, Egyptians all over the world created an island called Egypt in Second Life, a 3D virtual world, where they included avatars carrying signs supporting Egyptian protesters (Andrews, 2012).

When the Internet got restored in Egypt, activists around the world helped Egyptian citizens to cover their Internet activity and physical location to avoid retaliation of the Egyptian government (A. Russell, 2011). The use of the Internet by journalists, news organizations, and individuals created a networked system that allowed social awareness of what was happening during the Arab Spring (Papacharissi & de Fatima Oliveira, 2012). Social media became a coordinating tool for several world political movements to capitalize and organize political action, and this is the reason why authoritarian regimes try to limit populations' access to it (Howard & Hussain, 2013; Shirky, 2011).

2.1.4.3. An Overview of the Internet Shutdown during the Arab Spring

This subchapter provides an overview of the attempts to shut down the Internet in three nation-states part of the Arab Spring: Egypt, Libya, and Syria. Although first attempts to shut down the Internet occurred in Nepal and Myanmar (2005-2007), these two nation-states had an Internet penetration rate of barely one percent. In 2009, China concentrated its efforts only on one province,

Xixiang, while claiming reasons of national security (Economist, 2013). It was not until the shutting down of the Internet in Egypt that the world realized that the Internet from a nation-state could be separated from the global Internet (Thompson, 2012). Libyan and Syrian governments would shut down the Internet to prevent the downfall of their political leaders, despite the fact that the Internet penetration rate was lower than in the Egyptian case and that the Internet infrastructure was less developed (OpenNet, 2013).

2.1.4.3.1. Egypt

The Arab Spring showed to the entire world how vulnerable the Internet infrastructure is in authoritarian regimes. Shortly after midnight, January 27, 2011, the Mubarak administration cut-off internal access to the Internet and connectivity from the global Internet traffic into Egypt. The purpose of the government was to stop the communication among activists who demanded political changes (Bowman & Camp, 2013). Similar situations occurred in Libya and Uganda also in 2011 and Syria between 2011 and 2013.

By January 29, 2011, 91% of Egypt's Internet was down (ISOC, 2011). As mentioned before, to get access to the global Internet, the local ISPs needed a gateway, which is a link to other ISPs outside of Egypt. Initially, the Egyptian government ordered the local ISPs to disconnect their services from all international connections to the Internet; otherwise, they would face commercial and personal risk. Events unfolded as described below (Cowie, 2011a):

1. Telecom Egypt (AS8452), the national incumbent, starts the process at 22:12:43.
2. Raya joins in a minute later, at 22:13:26.
3. Link Egypt (AS24863) begins taking themselves down 4 minutes later, at 22:17:10.

4. Etisalat Misr (AS32992) goes two minutes later, at 22:19:02
5. Internet Egypt (AS5536) goes six minutes later, at 22:25:10.

This sequence shows that few ISPs with unique Autonomous System numbers (ASNs) were being ordered to shut off all external activity. Once the "adjacent" autonomous systems (ASs) border router noticed a lack of action from the Egyptian ISPs, it took the IP prefix off its BGP list. In consequence, most internal networks in Egypt were disconnected, except one, Noor Group, which was connected to Egypt's financial market. This situation shows that in the case of smaller territories with few ISPs, shutting down the Internet almost can be accomplished with some planning (Subramanian, 2011). Vodafone, a mobile phone provider, resisted but finally was forced to comply (Bowman & Camp, 2013). Finally, the only Egyptian IXP was disabled, which severely damaged the Egyptian internal connectivity (Bowman & Camp, 2013; B. Johnson, 2011).

2.1.4.3.2. Libya

Demonstrations against Muammar El Qaddafi, the de facto ruler in Libya between 1981 and 2011, started in February 2011. By that year the Libyan government was in control of the entire telecommunications infrastructure (Bowman & Camp, 2013; Hill, 2011).

On February 22, 2011 (almost one month after the Egyptian Internet shutdown), after shooting two men in a rally, Internet activists called for a "day of rage" in Tripoli. The more Libyan demonstrations expanded, the more Internet access was restricted (Gonzales & Harting, 2011). As reported by Hill (2011), Qaddafi ordered the two mobile phone providers to disconnect their services and later on, he ordered the government-run telecommunications company to physically cut the backbone fiber optic cables that connected the east part of the Libyan territory with the

west part of that nation-state. This last action was a desperate attempt to stop absolutely all Internet connectivity.

2.1.4.3.3. Syria

In Syria, the outcome of the revolution started during the Arab Spring is still unknown as the civil war continues, and Bashar al-Assad remains as head of the Executive branch. Bashar al-Assad has been President from Syria since 2001, after receiving the government from his father, Hafez al-Assad, who was a thirty-year-dictator (Bowman & Camp, 2013; Johnston, 2016). Protests started in March 2011, and at that time the Syrian government controlled (and still does) the Internet service. The Syrian Telecom Establishment, a government-run ISP, provides Internet service for the Syrian territory (Cowie, 2014; Stack, 2011b, 2011a). However, instead of using the same methods that the Egyptian or Libyan governments did, the Syrian government used a more pervasive way to stop Internet activity by cutting off entirely electrical services (Preston, J., as cited by Bowman & Camp, p.13, 2013).

On June 3, 2011, a national uprising attempted to force the resignation of President Bashar al-Assad. In response, the government shut down the Internet. Similar actions would repeat on December 1, 2012, and on May 7, 2013. From August 29 to October 10, 2013, the Internet was down in the city of Aleppo (Cowie, 2014; Google, 2011). Besides cutting off electrical service, Bashar al-Assad ordered the government-run ISP to interrupt the Internet service. Disruption in the Syrian Internet traffic was more manageable than the Egyptian case because, just like Libya, Syria does not have an IXP. As a result of this situation, Internet activists moved to the Turkish borderline to get Internet access (Bowman & Camp, 2013).

2.1.5. Democratic Regimes

For democratic regimes, it is more difficult to shut down the Internet because they must balance the protection of the critical infrastructure, civil liberties and the exploitation of the economic potentialities of new information and communication technology. Democratic regimes must take into account a sum of interest aggregations, such as entrepreneurs, consumers, Internet users and human right activists (Giacomello, 2005).

Having different stakeholders also means that they act differently based on their interests. Therefore, besides the protection of the critical infrastructure, democratic regimes also justify their control actions over the Internet by fighting against what the society considers illegal, such as Internet fraud, identify theft, drug dealing and child pornography (Barth, 1997; Giacomello, 2005). However, despite these considerations, democratic regimes also have adopted extreme policies for Internet control without having evidence that they make critical infrastructure more secure (Schneidewind, 2010; Schneier, 1996).

2.2. Unitary Executive Theory

The U.S. Constitution created a single chief executive officer, the President, who is also the head of the government. This is called a "unitary executive." According to the defenders of the unitary executive theory, the founding fathers intended for the president to have complete control and authority over all aspects of the executive branch (S. G. Calabresi & Yoo, 2003; Waterman, 2009). As a matter of fact, as Waterman states, the theory's central assumption is that:

> "… any law passed by Congress that seeks to limit the president's ability to communicate or control executive branch relations is unconstitutional and therefore need not be enforced.

> The theory also posits that the president has the same authority as the courts to interpret laws that relate to the executive branch." (Waterman, 2009, p.8)

When it comes to officials appointed by the president, the theory establishes that: (1) The president can remove subordinate policy-making officials at will, (2) The president can direct the manner in which subordinate officials can exercise executive power and (3) The president can veto officials' exercises of discretionary executive power (S. Calabresi & Yoo, 1997).

Constitutional bases for such power are in the article two of the U.S. Constitution (See Appendix 1). In this regard, according to the U.S. constitutional law provisions that refer to the unitary executive theory, the president has the power to control the executive branch (Cannon, Jordan, Keller, & Feeney, 2005). Moreover, the unitary executive theory establishes that the president has, not only the power to control but also the responsibility for the maintenance of the executive branch. At the same time, the executive branch must be responsible to its chief executive, the president itself (Waterman, 2009).

This theory also claims that the president should be able to make the final decision regarding any agency rules, even if the U.S. Congress assigned rulemaking activities to the agencies. Although the Congress may have initial power to assign responsibilities to officers in the executive branch, the president has the ultimate authority over the policies to be created (Cannon et al., 2005).

The U.S. administration has used regularly the unitary executive theory to justify an expansive presidential power, especially during the George W. Bush administration. However, the use and existence of the unitary executive theory is controversial because of the boundaries of the presidential power and Congress's ability to limit the presidential discretion (Waterman, 2009). Some academics claim that the most difficult aspect of the unitary executive theory is not that the

president can claim exclusive presidential power, but that the president may argue that he has a constitutional power that cannot be limited by the Congress (Ku, 2010).

On this regard, Calabresi and Yoo argue that "all of our nation's presidents have believed in the theory of the unitary executive" (S. G. Calabresi & Yoo, 2008, p.4). They go even further by stating that: (1) the U.S. Constitution gives to presidents the power to control their subordinates as they have the power of the U.S. president, (2) the executive branch carries the opposition to any limits on the president's authority to control and execute federal laws and, that (3) a 'gloss' of the words 'executive power' has borne to allow the congress to create a "fourth" branch of the government out of presidential control (S. G. Calabresi & Yoo, 2008).

The use of the unitary executive model was a characteristic of the Bush administration. In 2002, Vice President Richard Cheney at the time, claimed that the administration would be "… dedicated to restoring the balance of powers in the system of separated powers to ensure that Bush would be able to fully exercise his rightful authority" (Rozell & Sollenberger, 2013, p.37).

The executive privilege is the main element of the unitary executive theory and is the defined as the power of the president and the high executive officers to withhold information and testimony from Congress, the courts and the public. This is a long-time recognized principle, established in constitutional theory, practice and legal documents and yet, not explicitly recognized by the U.S. Constitution. Frequently, only those who have compulsory power (such as congressional committees or special prosecutors) can set limits to the executive privilege (Rozell & Sollenberger, 2013).

On November 1, 2001, former President George W. Bush issued Executive Order (EO) 13223 that expanded former President Reagan previous EO to expand the scope of executive privileges to current and former presidents. Under Bush EO former presidents could assert

executive privilege over their own documents, even if the incumbent president disagrees. At the time, not even the Presidential Records Act of 1978 contained such a high standard. This action of the Bush administration was the target of strong criticisms because ordinarily when a president seeks secrecy under the terms of the executive privilege is because of reasons of national security, and not just to cover documents of past administrations. Bush EO remained in the system until 2009, when President Obama reversed it (Barber & Fleming, 2011; Rozell & Sollenberger, 2015).

In 2008, when Obama was still a candidate, he criticized George W. Bush's use of executive power. Concretely, Obama criticized Bush for his policies over civil liberties of terrorist suspects, for circumventing Congress authority and for centralizing power in the presidency. However, when the time came, President Obama was also blamed of embracing unilateral actions of his own (Barilleaux & Maxwell, 2017).

2.3. Theoretical and Research Framework: the "Securitization Theory of the Copenhagen School," a.k.a. Securitization Theory

For this study, the theoretical framework to be used will be the "Securitization Theory of the Copenhagen School," also known as securitization theory. This theory, which originates from international relations, assumes a constructivist approach. Securitization in international relations is the process through which nation-state actors construct different subjects as issues of security. As consequence, extraordinary means and a specific type of politics are used in the name of security to act towards those subjects. Therefore, it is important to know who can securitize and under what circumstances (Buzan, 1998). The basis of the Copenhagen school approach focuses on the process of taking an issue from a politicized, or even non-politicized stage, into the security

domain and considers the multiple factors surrounding the formation of the security policy (Buzan, 1998; Dunn Cavelty, 2008). The actual process of bringing an issue from a politicized space or even a non-one into the security domain is known as "securitization" (Waever, 1995).

Regarding the theory itself "… the study of securitization aims to gain an understanding of who securitizes (the actor) which issues (the threat subject), for whom or what (the referent object), why (the intention and purposes), with what results (the outcome), and under what conditions (the structure) (Buzan, 1998, p.32)".

The Copenhagen school argues that a security speech is an act, through which a securitizing agent creates one or more referent objects (related to the national interest). Governments must protect referent objects because their protection is a matter of national security. For example, the U.S. government cybersecurity policy is an example of an attempted securitization. Constantly either the Pentagon or the Department of defense (DoD) securitizes the impact of hacking on critical infrastructures, which are vital for the survival of the U.S. as a viable nation-state (Hansen, 2009). In this regard, the most referenced referent object is the nation-state itself, which in the context of national security policies is threatened in its physical or ideational survival and, therefore, has to be protected (Dunn Cavelty, 2008).

According to some academics, cyberspace has been securitized based on institutional developments starting with the establishment of the Commission on Critical Infrastructure during the Clinton Administration in 1996. The military refers to digital technologies as the "backbone" of the Revolution in the military (Dunn Cavelty, 2008; Hansen, 2009).

Different government authorities have turned their speeches into security ones. Such statements about securitization have been oriented to construct cyber issues as security problems, rather than political, economic, legal or technical ones (Hansen, 2009). Members of the military

and politicians tend to call something a cybersecurity problem because then that issue takes a higher priority within the government security discourse. This practice seems to be a characteristic and way of acting of all regimes, democratic and non-democratic (Hansen, 2009; Williams, 2003).

Following this tendency, since 1991 members of the U.S. military created the term *"cyber Pearl Harbor," "first war in cyberspace"* or *"cyber 9/11"* to refer to a massive and direct attack against the critical infrastructure (Hansen, 2009; Lawson, 2016; Reuters, 2013). Members of the press also use the term *"cyber gathering storm"* (Weinberger, 2013). Independently of the opinions of members of the government about a potential cyber Pearl Harbor, its parameters, this is what to damage precisely within the critical infrastructure and the extension of the damage regarding time and quantity, have not been clarified (H. Farrell, 2013; Lawson, 2016).

Back in 2013, members of the U.S. national intelligence warned that there would be a major cyber-attack against the U.S. critical infrastructure systems during the next two years that would result in long-term, wide-scale disruption of services, such as a regional power outage. As they referred, that event could be characterized as a "cyber Pearl-Harbor" (H. Farrell, 2013; Weinberger, 2013).

As far as this research was able to conclude, until the end of April 2018, (even after the DDos attack on Dyn, the alleged Russian hacking of the Democrat party system and the WannaCry ransomware cyber-attacks that affected 74 nation-states) (Bodkin, 2017; S. Jones, Sevastopulo, & Hille, 2016; York, 2016), there has been no cyber-attack recognized as a "cyber Pearl-Harbor" by members of the military or politicians in the U.S. or any other nation-state (Lawson, 2016). However, members of the military do insist that, at least in the U.S., there will be one soon (Gurdus, 2016).

Government actors involved in the securitization process (usually policymakers or military members), do not consider the potential consequences of labeling a wide range of issues as security

problems (Buzan, 1998). Even more, the existence of threats (real or not) may be used to justify breaking the rule of law whether it is a democratic or non-democratic regime (Buzan, 1998; Williams, 2003).

2.3.1. Units of Discourse in Securitization Arguments

The security-speech-act contains six elements involved in the actual security process (Buzan, 1998; Dunn Cavelty, 2008; Rothe, 2015; Williams, 2003):

1. Securitizing actor: the individual or individuals who "securitize" something by declaring it a "referent object". A securitizing actor is either a person or group who performs the security speech-act. These individuals share a set of basic beliefs and have resources to act. However, a speech act only can be performed by an actor in a high position; usually, government representatives in a position of authority who can create an argument about a threat to the referent object. In this regard, a securitizing actor must:
    a. Have both, authority and legitimacy to be heard and believed for the targeted audience
    b. Have the capacity to adopt measures to deal with the problem

    These conditions limit potential candidates for securitizing actors to leading politicians, bureaucrats, pressure groups and maybe scientific experts or technocrats.
2. Speech act or securitization speech: this is the "performative act" that creates a security problem. Concretely this act creates a notion of security and includes an existential threat to a referent object, a sense of urgency and a call for extraordinary measures to fight against

a threat. The speech-act is directed to an audience that the securitizing agent must convince to execute an extraordinary measure.

From now on, this dissertation will refer to the *securitization speech* as *"security discourse"* to facilitate the analysis.

3. Referent object: "Things that are seen to be existentially threatened and that have a legitimate claim to survive" (Buzan, p.36, 1998). There can be one or more referent objects; the referent object is part of the national interest or is the national interest itself and, therefore, its protection is part of national security strategies. The referent object may change through the years and depend on each nation-state.
4. The Audience: Person or group of people who need to be convinced with the security speech-act that there is a referent object (the things to protect to preserve the nation-state) and that its protection is part of the national security strategy. To convince audience the securitizing move creates a sense of urgency and legitimizes the adoption of a set of exceptional or extraordinary measures to deal with the security problem. Additionally, to convince an audience, the actor who performs the speech-act must be argumentatively persuasive.
5. Extraordinary or exceptional measure: Actions out of the ordinary to protect the referent object. Extraordinary measures depend on the context and are also very subjective.

According to the authors of the Copenhagen school, the process of "securitization" is linked to a "speech-act". This connection is the reason why some academics call this theory "speech act theory". The idea behind speech-act means that speakers use a type of language that includes propositions and statements with content (that may be true or false), but more important performances that conceptualize the notion of security beyond traditional points of view (Butler,

2007; Rothe, 2015). “Speech acts follow a conventionalized script to which the speaker has to stick and many are bound to the authorize position of certain speakers” (Rothe, 2015).

The distinguishing feature of the Securitization Theory is its rhetorical structure. In the security discourse, an issue is “dramatized and presented as issue of supreme priority” (Buzan, p.26, 1998); therefore, by labeling that specific issue as “from national security,” the agent claims an extraordinary treatment for that issue (Williams, 2003).

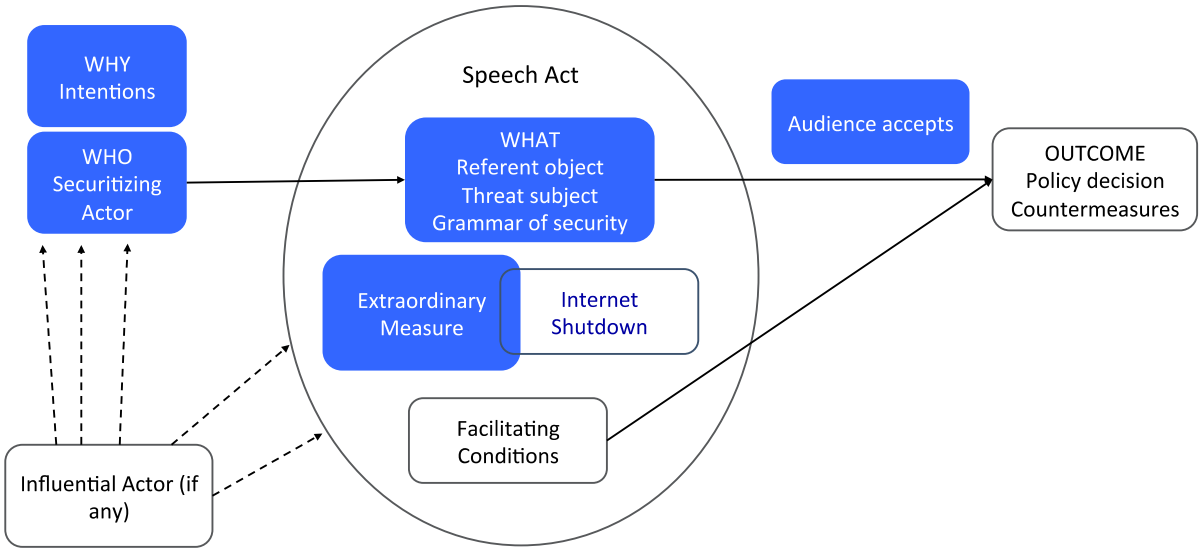
By referring to the urgency of action posed by an existential threat, a securitizing actor can transform an issue into one of security and can attempt to make anything a referent object. Traditionally, the referent object is the nation-state, threatened to its “physical or ideational survival,” and therefore, it is in need of protection (Hansen, 2009). However, the security discourse may create different referent objects, other than nation-states and bring in other sectors than the military.

The Copenhagen school states that there are two conditions to facilitate the securitization process (Buzan, 1998):

1. The speech act follows the grammar of security, this means, it constructs a plot containing an existential threat and makes an argument of no return and offers a ‘securitized’ way out
2. The securitizing agent holds a position that allows creating an authoritative claim about security

Using the terms of the Copenhagen school, this study explores the circumstances different regimes have used to justify shutting down the Internet as an “extreme measure” to protect what they consider the “referent object”. In this regard, I will identify who the securitizing agents are, why they say they want an Internet shutdown or why shut down the Internet, what the referent object is and the audience they attempt to address (Please see figure 05).

Figure 05.- Copenhagen School Securitization Theory Basic Diagram and the Internet Shutdown



Modified from Dunn Cavelty, p.28, 2008

2.4. An Overview of the Literature and Opportunities for this Research

The academic literature divides current studies about attempts to shut down the Internet in two types:

1. From a legal point of view, legal scholars analyze three bills proposed by U.S. Senators to grant powers to the president to shut down the Internet within U.S. territory (Bambauer, 2011; E. Fischer, 2012; Medows, 2012; Ruggiero, 2012; P. Shane, 2012; Thompson, 2012). The discussion focuses on whether section 606 of the Telecommunication Act of 1934 gives to the U.S. President the capacity to take over all telecommunications within U.S. territory (Opderbeck, 2012, 2013). Some of these studies were enriched by performing a historical analysis of the evolution of the telecommunication system in the U.S. and its corresponding national security policy. These studies however, are limited to legal analysis

of whether shutting down the Internet would be legal or not within the U.S. system. There was no further research on the status of the Internet infrastructure or political reasons to shut down the Internet. The analysis is also limited to the U.S. only and does not consider other democratic or hybrid regimes.

2. From a social sciences and historical point of view, academics present as part of the context about Internet shutdowns multiple studies about the Arab Spring cases, the case in Nepal back in 2005 and the use of the Internet as a tool for political change. I will describe these studies below, but it is essential to clarify that, although this study considers the Arab spring as part of the global context when talking about Internet shutdowns, this political phenomenon is not under analysis. Nation-states involved in the Arab spring, alongside with Nepal, belong to the group of "authoritarian regimes," which are not part of this study.

Literature about the Arab Spring cases (Egypt, Syria, and Libya) focus in the historical aspects of the Internet shut down, precisely how the past events unfolded since the specific circumstances that trigger national protests until the Internet was shut down and later restored. Concretely the literature pays particular attention to two particular issues: 1) the efforts of the population to bring the Internet service back (Andrews, 2012; Bowman & Camp, 2013; Dunn, 2011) and 2) the role of the social networks as a catalyst or strategic tool in the revolution that overthrew Mubarak's administration (Khondker, 2011; Tufekci & Wilson, 2012) (Harlow & Johnson, 2011b; Howard & Hussain, 2013; Tufekci & Wilson, 2012).

In the specific case of Nepal, shutting down the Internet was included in a study as part of the strategy of the government to stop all telecommunication activity and isolate Nepal from the rest of the world in 2005 (Ang, 2012). The study concludes that shutting down the Internet in Nepal, like in Egypt, did not only contribute to the purposes of the authoritarian regime but that it

had the opposite effect. Those who were apolitical became political against the government, and those who saw their business affected also turned against the authoritarian regime (Ang, 2012; Hassanpour, 2014).

Finally, as mentioned before, when describing the Arab spring, a group of academics credit the Internet with being the catalyst for political changes. For the events of the Arab Spring, they conclude that the Internet became a tool to mobilize pro-democratic movements and lead a revolution. According to this academic research, such events of mobilization and further revolution, were possible thanks to the existence of significant communication platforms, such as Facebook, Twitter, and YouTube (Harlow & Johnson, 2011b; Lotan & Graeff, 2011).

There is, however, another set of scholars for whom the Internet should not be credited with the civil awakening of new generations. According to Anderson (2011) political movements like the Arab Spring happened before at the beginning of the twentieth century when the Internet did not exist. For Anderson, what is required to conduct a revolution like the Arab Spring is the way organizers influence the local contexts at the point of organizing an uprising by using any means to their disposal, either the Internet or traditional word of mouth in homes and mosques (Anderson, 2011; Tufekci & Wilson, 2012).

So far, all these studies address the Internet shut down in these conditions:

1. Legal studies in one consolidated democratic regime (U.S.)[11] analyzing telecommunications statute and bills drafted within the legislative branch.
2. Political studies about the role of the Internet in the development of a revolutionary process such as the Arab spring

[11] By the beginning of 2017, the Economist Intelligence Unit (EIU) reclassified the U.S. from being a consolidated democracy into a "flawed" one and Russia was reclassified from being a hybrid regime into an authoritarian one (EIU, 2017)

3. Political studies that focus on authoritarian regimes, not only the ones included in the Arab spring but also the earliest Internet shut down, Nepal. These studies analyzed the role and participation of the government trying to control the Internet infrastructure, but do not study other potential participants such as civil society, the private sector or the population. The role of civil society is, to some extent, analyzed in the studies about social networks.

The current project takes a different approach from the previous ones concerning the type of study, type of data, actors involved and academic approach. This study includes:

1. The analysis of nation-states considered well-consolidated democracies and hybrid regimes (differently from the authoritarian ones and the cases of the Arab Spring). Existent studies that focus on hybrid regimes cover government policy to act over the Internet infrastructure (Nocetti, 2015; Vendil Pallin, 2017) but do not address Internet shutdowns specifically
2. Besides the legal analysis of just one particular statute, this study will include a description of the following aspects of each case-study: status of the Internet infrastructure, powers of the executive branch in the selected case-studies, economic context, drafted bills alongside with broader legal and constitutional frameworks and political justifications of why shutting down the Internet was necessary (for the regimes that did it). or would be necessary (for the ones that considered it)

The Securitization Theory is an appropriate theoretical framework because it facilitates the analysis of different elements not contemplated in previous academic work. Although the extreme measure, an Internet shutdown, remains the same among all case-studies, the new items to analyze include: 1) new actors, other than members of the executive branch (f/e different parties in the private sector, members of the military and owners of the Internet infrastructure), 2) the audience

and why it is crucial (this will depend on each case), and 3) different notions of the concept of national security and national interest, which rely on the specific legal and geopolitical context of each case-study.

Finally, this study will give a step beyond the theoretical framework and previous academic work. This study identifies the legal, political and technical factors that enable a consolidated democratic or a hybrid regime to shut down the Internet, beyond the justifications different governments may provide.

3. Methods and Research Design

This chapter introduces the methods and procedures of the proposed study, including research design, selection of case studies and justification for choice, data collection and description of analysis.

This research is a comparative multiple-case study, which examines (1) the global scope of the Internet shut down activity, (2) government security speeches of hybrid and democratic regimes that justified shutting down the Internet or considered doing it in selected case-studies and (3) the actual reasons why hybrid and democratic regimes shut down the Internet or considered doing so also in selected case-studies. In this context, this dissertation understands as security speeches a set of spoken or written statements that are significant in a security framework (Securitization Theory in this case). Actors in position to define nation-state security policies and to propose actions or responses against envisaged threats are the ones that perform the security speeches (Dunn Cavelty, 2008)[12].

The government action under discussion in this case is the Internet shut down or considerations to do it under circumstances of national security. Actors who perform the speech, are presidents, prime ministers, ministers, senators, members of government agencies, administrative regulators' members, policymakers, bureaucrats, and academics. These are public people in their nation-states, and their statements are available as general information on the Internet.

[12] Differently political speech is defined as set of expressions, written or spoken, that comment about one or more government actions or expected actions, that are both intended and received as a contribution to public deliberation (Holmes, 2013).

3.1. Qualitative Research

This study follows a qualitative research design. Qualitative methods are widely used in the social sciences and also in policy evaluation (Hoefer, 2012). The fact that data may be collected over a sustained period makes it more powerful for studying processes, especially in historical analysis (Miles, 1994). The term 'qualitative' suggests a deep analysis or emphasis on the qualities of the entities and processes under study, differently from the intensity measurements of the quantitative methods. When the study involves a qualitative case study, the research approach facilitates the exploration of a phenomenon within its context using a variety of data sources. By following this technique, we make sure to explore the issue under study through multiple lenses, a process that allows discovering different facets of the phenomenon (Baxter & Jack, 2008; Denzin, Norma; Lincoln, 2005).

3.2. Recap of Research Questions and an Overview of the Research Design

This dissertation has three purposes, which are reflected in the three research questions (RQ) mentioned before:

RQ1: What is the global scope of the Internet shut down phenomenon?

RQ2: What justifications do democratic and hybrid regimes use to shut down or to consider shutting down the Internet?

RQ3: What are the political, legal and technical factors that drive a government to shut down the Internet?

The first purpose (RQ1) is providing the global scope of the Internet shut down phenomena. As it will be explained later, with that goal in mind, I conducted an intensive effort to collect all relevant security discourses by public officials and legal documents in and on select cases (this is detailed further below). For that purpose, I used keywords to identify potential and reliable sources of information. Additionally, this section will also explain the main problems this research encounter during this process.

To answer RQ1, we documented all known instances of considerations or execution of government shutdowns of the Internet across the globe using publicly available materials. Those materials include news accounts, citizen accounts via blogs, international organizations, reports, and other social media, as well as legal or policy documents written by governmental actors and agencies. All this information was triangulated.

The second purpose of this dissertation is identifying the rhetorical justifications that democratically organized governments and hybrid regimes provide when considering or executing an Internet shutdown (RQ2). The second question focuses on understanding the broad and narrow arguments governments create to justify an Internet shutdown. For this question, I focus on the rhetoric. Prior academic research indicates that the security discourse of democratic regimes explains government control over the Internet infrastructure as necessary to protect what they call the national interest and to fight against cybercrime, child pornography, and computer frauds (Giacomello, 2005). However, as I will illustrate in this document, a uniform definition of what the national interest is for these regimes does not exist.

Shutting down the Internet has been considered a remedy for different situations that threaten the national interest because the protection of the national interest guarantees the survival of the nation-state (Richards, 2012). The aim of this dissertation is examining more closely those

arguments since governments "construct" the concept of national interest and potential threats (Katzenstein, 2003). In doing a close analysis of the rhetoric produced by governments, I determined the differences between hybrid and democratic regimes in building their arguments about national security when the Internet infrastructure is involved.

To answer RQ2, I analyzed the speeches using the theoretical framework of the securitization theory of the Copenhagen School. For this dissertation, the unit of analysis is the securitizing agent speech that was created to convince an audience that shutting down the Internet is necessary for national security purposes. The securitization theory defines an agent according to his/her position as a leading politician, bureaucrat or representative of a government agency during a specific time. The security discourses of these agents contain what we want to know, the rhetoric of the justifications different regimes use to shut down or to consider shutting down the Internet.

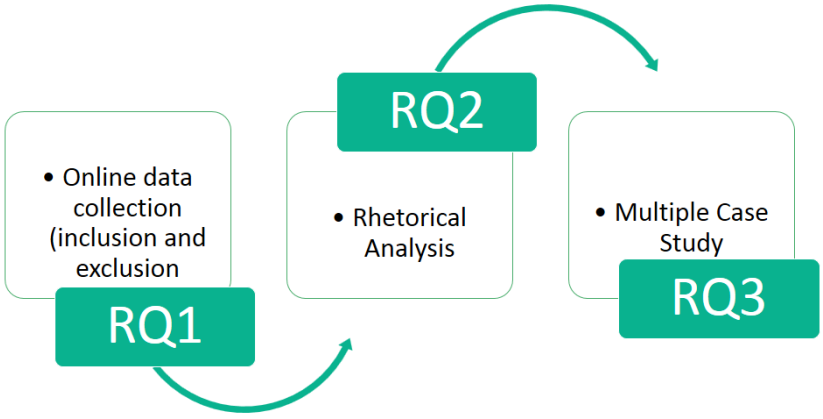
Regarding RQ3, the purpose of this question is identifying the political, legal and economic factors that enable democratic and hybrid regimes to shut down the Internet or to consider doing so. With this goal in mind, this document contains a description of multiple case studies and detail of political and legal systems, telecommunications infrastructure, and critical historical or current events to understand the factors that lead to considerations of government authority over Internet access by citizens in a nation-state. Description of the case studies also reports efforts of their governments to control the Internet infrastructure within their territories. Figure 06 contains a visual representation of the research design this dissertation has followed.

RQ3 looks closely at the structural factors that enable an Internet shut down or the consideration of it in democratic and hybrid regimes. With this purpose in mind, this dissertation conducted a comparative case study and included cases of democratic and hybrid governments

that have not considered or executed an Internet shutdown. By doing this, it is expected to isolate better vital structural factors that differentiate regimes that are inclined to exert the ultimate control of government authority as compared with those that are not.

The academic literature defines a case study as a phenomenon of some sort occurring in a bounded context (Miles, 1994; Yin, 2009). Case studies may be individuals, organizations, small groups, roles, communities, nation-states, and unique events, among others. As Yin suggests (2009), research may be conducted with single or multiple case studies. Single case studies may be helpful especially if they are extreme or unique. Extreme or deviant cases have unusual manifestations of the phenomenon of interest, which is why they are relevant (Bailey, 2007). Concerning policy analysis, the use of multiple case studies or comparative case studies is a way to create policy options and also provides an opportunity to learn from the experiences of a group of nation-states regarding the same practice (Horvath & Daly, 1989).

Figure 06.- Graphic Representation Research Design



3.3. Online Data Collection: Inclusion and Exclusion Criteria

The first step to identify Internet shutdown cases at a worldwide level was conducting an Internet research process considering inclusion and exclusion criteria for the search. The exclusion and inclusion criteria helped to identify multiple sources and to triangulate the data (Fink, 2010; Ridley, 2008). A search was conducted in different databases and different search engine, as described in table 02. This dissertation tried to include all possible points of view: governments, the private sector, civil society, and academia.

Table 02.- List of Sources Used to Gather Data

Type of Data	Identified Sources
1. News, articles, websites, blogs, and related artifacts (like videos, podcasts, and social media platforms) related to the participation of private telecom operators or government actions over private Internet infrastructure. 2. If available, speeches of securitizing agents (which are security speeches)	*Academic websites:* OpenNet Data Initiative, Belfer Center, MIT Technology Review, Berkman Klein Center (Harvard University) *Academic Databases:* LexisNexis Academic, Web of Sciences *Government sources:* Congress.gov (U.S. Congress), APH.GOV.AU (Parliament of Australia), GOV.UK (U.K. Parliament), KREMLIN.RU (President of Russia-Kremlin), PRAVO.GOV.RU (Official Internet portal Legal Information, Russia), ASOZD2.DUMA (Duma Legislative System, Russia), www4.PLANALTO.GOV.BR (Portal Planalto, Brazil), www.DIPUTAODS.GOB.MX (Cámara de Diputados de la Unión, Mexico), www.SENADO.GOB.MX (Gaceta del Senado, México), www.OAS.org (OAS Cyber) *Private Sector and Civil Society:* Dyn (former renesys, Measure of the Internet Performance), BGP Monitoring the Internet, Akamai Technologies, Akamai, CloudFare, InternetIntelligence, Internet Society (ISOC) *Search engines (Google, Yahoo, Ecosia, Bing):* provided additional sources: Electronic Frontier Foundation (EFF), RT, Renesys, The Economist, The Moscow Times, Vedomosti, BBC, BBC America Latina, The Guardian, The Washington Post, New York Times, Lawfare Sputnik, Foreign Policy, Foreign Affairs, Financial Times, Ars Technica, Computerworld, ZDNet, WIRED, CNET, Instituto Federal de Telecomunicaciones, El Universal de Mexico, Meduza in English, American Enterprise Institute (AEI), Quartz, other alternative sources

I developed an inclusion criteria using the following keywords individually and in combination: Internet, "Internet shut down," "Internet kill switch," "Internet blackout," "kill the Internet," "cut off the Internet" government control over the Internet infrastructure, ["Internet shut down" AND "cyber security policies"], ["Internet kill switch" AND "cyber security policies"], ["Internet blackout" AND "cyber security policies"], [Internet shut down AND "Internet governance"], [Internet shut down technique], [Internet outage" AND "Internet governance"], [Politics of an Internet shut down] and [Economics of an Internet shut down]. After identifying these keywords, I conducted a search process in three languages: English, Spanish, and Portuguese without any assistance. As part of the search process, I add Turkish and Russian; this final stage required the help of third parties and software assistance.

Exclusion criteria were based initially only concerning time. The parameters to collect data started in 1991, the year when the World Wide Web (www), also known as the Web, became available to the public. The www and the Internet are not the same; the www is the most popular "part of the Internet" and the one that is most accessed by Internet users. Although they are not the same thing, Internet users in general think of both terms as the same thing (Beal, 2010)[13]. Results of the search also included academic papers and books. A quick review of abstracts or introductions was helpful to determine whether they should be included or excluded. I scanned Web pages before incorporating or discarding them. This process allowed me to identify the first Internet shutdown: Nepal in 2005 during a time of national protests. After determining that episode, I narrowed the timeframe to start looking for sources in 2005 and after.

[13]As described at the beginning of this dissertation, the Internet is a massive network of networks that connects millions of computers together. Any computer can communicate with another one if they both are connected to the Internet. The World Wide Web (www) is a way of accessing the information available on the Internet. The Web uses the HTTP protocol, to allow applications to communicate to share information. The Web also utilizes browsers, such as Internet Explorer or Firefox, to access Web pages that are linked to each other. The web is just one of the ways that information can be distributed all over the Internet. The Internet (not the web), is also used for email, instant messaging and FTP (file transfer protocol) (Niedrich, 2011).

The literature about Internet shut downs increased between 2009 and 2011, presumably for two reasons: 1) the securitization policy of the cyberspace in the U.S. and 2) the Arab spring. However, since 2014, concepts became a challenge. In that year, and mostly from the perspective of civil society organizations, the use of the term "Internet shut down" started referring indistinctly to the shutdown of the entire Internet and the episodes of censorship. The last ones only affect specific web pages or applications, such as Facebook, Twitter or WhatsApp (accessnow, 2017). In accordance to the definition explained in the first chapter of this dissertation, stopping or blocking the traffic of specific web pages of applications is a case of "technical blocking," which is a form of censorship, but not an Internet shut down.

Because of the inclusion and exclusion criteria, the conclusions of this dissertation are the result of the analysis of approximately 4,105 different sources of data. Although until 2013 there were no academic publications about Internet shutdowns after that year publications appeared mostly referring to authoritarian regimes.

Finally, because this dissertation relies upon documents available on the Internet, before including any actual statement of a potential securitizing agent as part of the data to analyze, the same account had to be available in at least three different sources that did not refer each other. Then I triangulated the data, a process necessary to trust in the validity of the conclusions (Miles, 1994).

3.4. RQ1: Selection of Internet Shutdown Cases

As explained before, this dissertation concluded that Internet shutdowns started in 2005 in Nepal by an authoritarian regime. However, consolidated democracies and hybrid regimes have

also been active in the debate and have considered creating techniques for a potential Internet shut down.

The process to determine whether a case is an Internet shut down is as follows:

1. I discarded cases where only applications were affected. As mentioned before, it is the point of view of this research that stopping or blocking the traffic of specific web pages of apps is a case of censorship. Therefore, if the source under analysis only reports episodes related to applications, that source is discarded.
2. When I identified the report of a full Internet shutdown, then the study of the information included some of the elements mentioned in the first chapter when the technical aspects of an Internet occurred: a) the status or situation of the ISPs (what are their statements? Were they threatening to stop the Internet service? Are there claims of an accident?), b) Governments' statements (what is going on?), c) Political opposition statement (if any), d) Claims of the population, mainly Internet users (did they lose access to the entire Internet or just some applications?), e) If the international Internet activity cannot be accessed, it means the DNS has been affected or poisoned and f) information available about IP address ranges falling off the Internet, situation known as the "Internet prefixes down".
3. The last situation mentioned in item 2, when the Internet prefixes are down, this means that the BGP has been affected, which also means that ISPs cannot connect to each other and that Internet users have problems connecting to different ISPs. If the nation-state has one or more IXPs and ISPs cannot connect each other properly, this means that IXPs have been affected at least partially.

4. Finally, the last analysis includes cases where there was not an Internet shut down, but there was a political, legal or academic debate on the subject. This dissertation calls these cases as “consideration to shut down the Internet”.

3.5. RQ2: Rhetorical Analysis. Classifying Data According to Codes

This document conducted a rhetorical analysis of security discourses related to the practice of shutting down the Internet or considerations to do it, in selected case studies and when those speeches were available. Security speeches are available in news articles, websites, blogs, and related artifacts (like videos, podcasts and social media platforms) about the control over the Internet infrastructure.

To analyze speeches as a rhetorical act, Campbell (2009) suggested the following categories:

1. Purpose: The conclusion, final product of the discussion, also known as thesis and the answer desired by the rhetor (For this case, I will use the term rhetor as a synonym of the speaker).
2. Audience: The receivers of the rhetorical act; this could be an intended audience, target audience or specialized audience. For this dissertation, I will focus on what Campbell calls “agents of change” and the “targeted audience”. The first audience (agents of change) facilitates the changes and measures the securitizing agent requires. The second audience (targeted audience) influences the security discourse, even if does not agree with it.
3. Evidence: Material support to build the argument

4. Strategies: The adaptation of all the above, including language, appeals, and discussions to shape the materials to overcome the challenges the rhetor faces

These elements are always present, and they are essential to understanding how rhetors use, write, speak or use visual messages to invite others to assent to social truths (Campbell, 2009). These categories will provide additional elements for judging the constructions that political actors are making about national security events and the rationalizations of shutting down the Internet.

In practical terms, the collected documents for this project were coded and analyzed following the previous categories (purpose, audience, evidence, and strategies) by using computer-assisted qualitative data analysis software (ATLAS.ti). The process of coding consists of classifying data into themes and codes by closely examining the data itself (Babbie, 2017). To achieve the final conclusions, I conducted three rounds of data reading and organizing in a period of one and a half years. Since the phenomenon of shutting down the Internet continues over time, I continuously update the data under analysis to answer RQ1, the global scope of the Internet shutdowns episodes. In the process of coding, we continuously used a careful interpretation to validate existing theories by providing descriptions of a particular phenomenon (Miles, 1994).

As mentioned before, the coding process followed the categories of the rhetorical analysis and used the Securitization Theory as a theoretical framework. Following a deductive approach, this dissertation started with a proposition, which was that democratic or hybrid regimes shut down the Internet or consider doing so because of reasons of national security (Babbie, 2017; J. Creswell, 2003). To have an accurate idea of the security speech to be analyzed, I separated specific sentences under quotations from the rest of the text, so I could understand what rhetors were saying. Accuracy of the statements was secured by triangulating the data. The rhetorical analysis

turned to be very helpful to understand the way security discourses construct a security speech when they address the problem of an Internet shutdown.

3.6. RQ3: Comparative Case Study

Case studies are part of a research process related to a person, a group of people or a unit. The purpose of a case study is to get conclusions over several units and generalize results. Another definition considers a case study as the analysis of systems to be studied with a comprehensive view, using one or several methods. Given this definition, the case study method is an appropriate way to explore a setting to understand it (Cousin, 2005; Thomas, 2011). However, Creswell provides a broader and comprehensive definition of what a case study is:

> "The case study method "explores a real-life, contemporary bounded system (a case) or multiple bounded systems (cases) over time, through detailed, in depth data collection involving multiple sources of information… and reports a case description and case themes" (J. W. Creswell, p.97, 2013).

A crucial decision for a research project is whether to conduct one or more case studies. The second option is known as a comparative or multiple case study. The most important difference between a single case study and a multiple case study is that when there are various cases, researchers have the opportunity of identifying similarities and differences among cases. In this context, the data can be analyzed within each situation and across situations. Comparative case studies also allow to create or test a theory when the suggested cases are well grounded in several empirical evidence (Baxter & Jack, 2008; Yin, 2003). In general, the evidence of multiple case studies is considered more compelling and the research study more robust. By identifying

similarities among case studies, these patterns would provide substantial support for the initial proposition or hypothesis (Yin, 2014).

3.6.1. Why a Comparative Case Study?

A comparative case study is preferred because it provides a better understanding of diverse processes and outcomes (Miles, 1994). More critical, case studies provide unique insight into areas where few studies or none have been conducted, such as with the phenomena of shutting down the Internet (Benbasat, Goldstein, & Mead, 1987). Except for very few legal analyses of U.S. bills created between 2009 and 2011 to grant powers to the U.S. president to decide whether the Internet should be shut down or not, little legal or social analysis exists to document democratic and hybrid governments' efforts to implement an extreme policy of government control over the Internet infrastructure.

Although case studies have been used to test hypotheses in quantitative research and to generate theories, they are also useful for exploratory, explanatory and descriptive studies (Tellis, 1997)[14]. This characteristic of case studies is an asset, considering that this dissertation is mostly exploratory but partially explanatory. It is expected to explain the rhetorical justifications governments use when considering or executing an Internet shutdown, as well as to identify the institutional and structural factors that might help to predict future Internet shut down events. In this sense, the case study represents an ideal methodology for in-depth investigation (Tellis, 1997).

[14] As defined by Yin (2009), case studies may be:
a) Exploratory cases: usually considered a prelude to a deeper social sciences research
b) Explanatory cases: used for causal investigation (that is why they are used for quantitative studies)
c) Descriptive cases: they require a descriptive theory to be developed before starting the project.

To be more critical about the validity of the study and generalize the results, the sampling process, which includes settings, actors, events, and processes, becomes a crucial point of the research design (Miles, 1994). It is important to clarify that for RQ1, there are no selected cases, but all known practices of Internet shutdowns between 2005 (when the first Internet shut down was reported) and early 2018. I established the instances for RQ2 and RQ3 from an earlier study that identified consolidated democracies and hybrid regimes that shut down the Internet or considered doing so (Vargas Leon, 2015) and with the online searching process I conducted for this dissertation. To understand governments' arguments for shutting down the Internet, selected cases include those that have provided a public reason or legal documents that can be analyzed. RQ3 attempts to understand the factors or characteristics that relate to shutting down the Internet. With this purpose in mind, cases under analysis must include governments that shut down the Internet and considered doing so, and instances where governments did not, to make a comparison (Please see table 03 in the next page).

The selected case studies for this dissertation were grouped into categories of types of government regimes (consolidated democracy, young democracy, and hybrid), according to the literature on regimes of the Economist Intelligence Unit (EIU) classification. All the selected cases have been involved, to some extent, in multiple episodes of government control within the last twelve years.

I selected the case studies for this research following the criteria I explain in the next paragraphs. Items 1 and 2 describe the selection of consolidated democracies; items 3 and 4 illustrate the choice of hybrid regimes:

1. In case of consolidated democracies, the cases under study are the only ones this study identified as the ones where an Internet shut down occurred or was considered legal, politically or even academically: Australia, U.K., and the U.S.

   As far as this research could identify there are no additional consolidated democracies that were involved in an Internet shutdown or considerations to do it
2. I compared consolidated democracies with young democracies: Brazil and Mexico. Young democracies are the ones that, although they exercise some level of control over the Internet infrastructure (as consolidated democracies do as well), lack a discourse or practices in favor of shutting down the Internet or to considering doing so. Brazil has denied the possibility of any actions of this kind, and Mexico even grants constitutional protection to the Internet infrastructure. I will address these facts adequately in the next chapters
3. In case of the hybrid regimes, something similar occurs. The cases under study are the only ones this study identified as the ones where an Internet shut down occurred, Venezuela, or where an Internet shutdown was considered, Russia. As far as this research could distinguish there are no more hybrid regimes that shut down the Internet or considered doing so.
4. The Economist Intelligence Unit (EIU) classification does not make a distinction within hybrid regimes as it does for democracies (between consolidated and young ones). Therefore, for this case, as a case to compare with Russia and Venezuela, this research uses the Turkish government. Turkey is a well-known case of a government that exercises high levels of control over the Internet infrastructure, by blocking social networks and poisoning the DNS, but never shut down the Internet. I will address these facts will be properly in the next chapter.

Selected case studies, previously mentioned, are detailed in the table below:

Table 03.- Selected Case Studies and their Particular Characteristics						
Nation-State	**Consolidated Democracies**	**Young Democracies**	**Hybrids**	**Internet Shut Down**		
				An Internet Shut Down Occurred in this Territory	**Governments never Considered Shutting Down the Internet**	**Governments and civil society conducted a political, academic or legal debate on the subject**
Australia	x			x		
U.K.	x					x
U.S.	x					x
Brazil		x			x	
Mexico		x			x	
Turkey			x		x	
Russia			x			x
Venezuela			x	x		

The purpose of this distinction is to find out why similar regimes act differently. For example, consider two hybrid regimes, Venezuela and Turkey. The first one shut down the Internet, and the second one did not. By identifying the circumstances of why one shut down the Internet, and the other did not, it will be possible to determine the factors that lead a government to shut down the Internet or to consider doing it and the ones that may prevent a government of using this practice.

At this point, it is important to remember that the proposition for this project is that all regimes, whether they are democratic or hybrids, shut down the Internet or considered doing so under the justifications of a national security situation. However, as I will depict in the next chapters, what each government understands for national security may be very different from others, even if they are politically similar regimes.

By having this comparative case study, it is possible to determine what government considers the national interest, that thing that must be protected to guarantee the survival and stability of a nation-state. By identifying the national interest, it is possible to identify the main elements of the national security policy of a government and the reasons why that government could consider shutting down the Internet.

3.6.2. Australia

Australia is considered a consolidated democratic regime, an OECD[15] (Organization for Economic Co-operation and Development) member, a federal parliamentary constitutional monarchy and member of the common law. Australia is also one of the most stable and prosperous economies in the world (Conversation, 2013; EIU, 2017; OECD, 2014). Nevertheless, despite being a consolidated democratic regime (EIU, 2017), Australia has been involved in multiple cases of censorship and is highly dependent on one major ISP, Telstra Corporation Limited, known merely as Telstra (Hernandez, 2014).

In 1994, the Australian government considered imposing restrictions over the Internet content. In that year, the Department of Communications and the Arts released a document titled "Regulation of Computer Bulletin Board Systems". This report detailed a list of actions and content that was considered harmful to minors and recommended to restrict similar kinds of content through self-regulation (Sorensen, 1996; Subramanian, 2011).

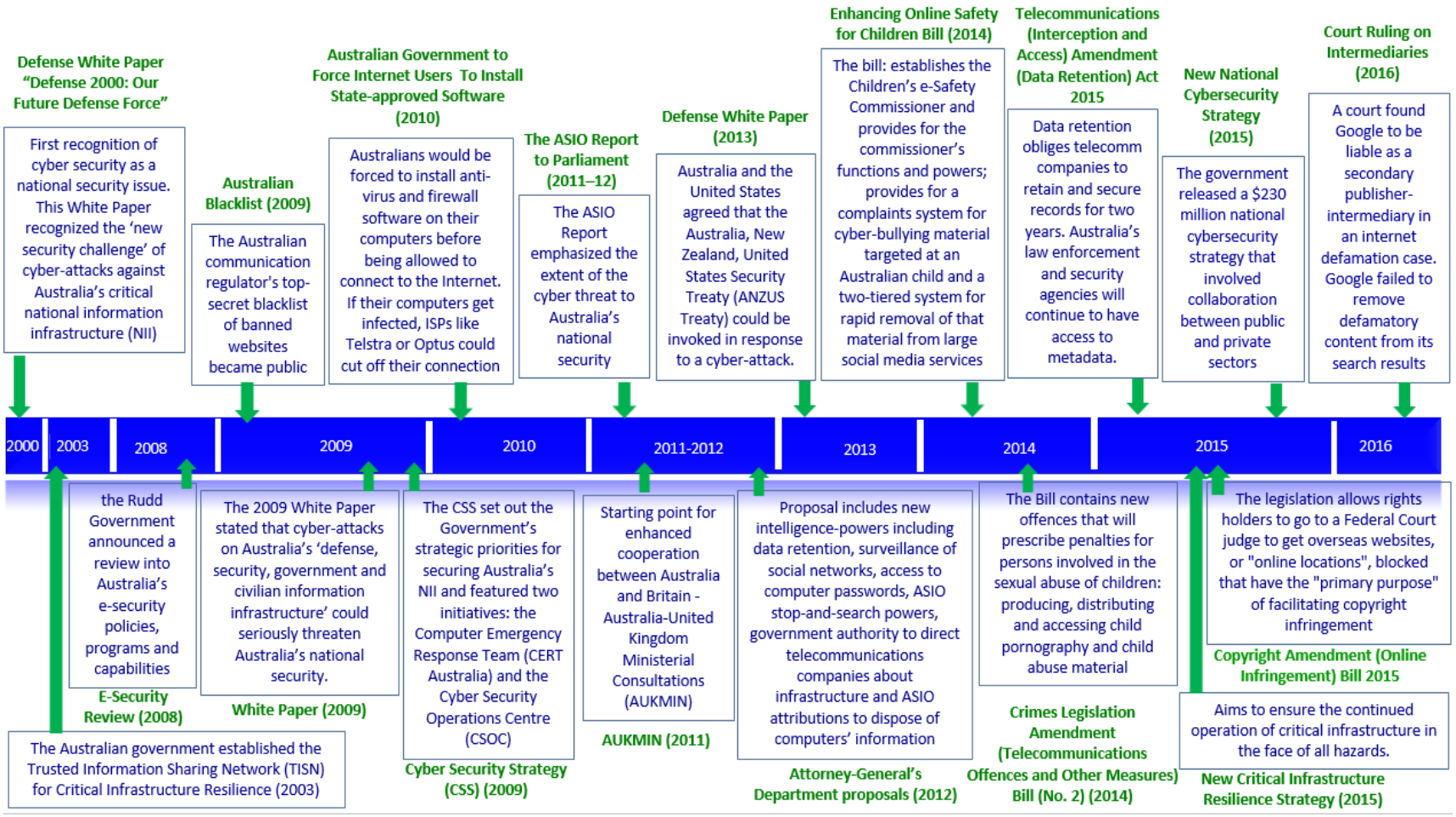
[15]The Organization for Economic Co-operation and Development (OECD) is an inter-governmental organization formed by 35 nation-states, all of them democratic regimes. Created in Paris, France in 1961 the mission of the organization is to promote policies that will improve the economic and social well-being of people around the world. OECD standards for policy matters and quality of life are considered a referent for most democratic regimes all over the world (Beal, 2010).

Since the year 2000, when cybersecurity became a national security issue, the Australian government started to produce laws of censorship and control over the Internet infrastructure (Singel, 2009). On December 31, 2007, Stephen Conroy (at the time Minister for Broadband, Communication and the Digital Economy) announced the federal government's new policy to censor "inappropriate material" from the Internet. According to this new system, any Australian who subscribes to an ISP would receive a “version” of the Internet, previously approved by the government. Justifications for this new policy were related to the protection of children from accessing violent and pornographic websites. Later, the Australian government abandoned this policy. However, they continue censoring sites that violate Australian laws (Deibert, Palfrey, Rohozinski, & Zittrain, 2010).

Three years later, in 2010, the Australian government created strong Internet censoring policies (LeMay, 2010a). Moreover, when state elections took place, Internet bloggers and anyone commenting on the state election in South Australia was required to publish their real name and postcode when commenting on the poll (Blair, 2010).

Since 2006, the legal production of cyber security white papers (the Australian term for bills), reviews, and strategies has increased in Australia, alongside with amendments to the telecommunications statutes of that nation-state and individual actions of the government over the telecommunications infrastructure. To have a comprehensive idea of these elements, please see figure 07.

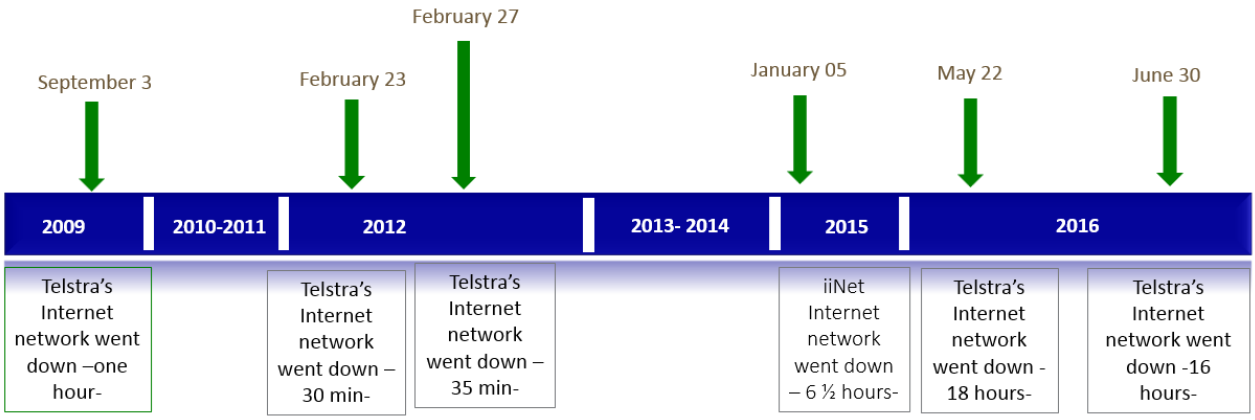
Figure 07.- Australian Bills, Actions, and Laws about the Internet Infrastructure (2000-2016)



Thinking about the Internet shutdown in concrete, Australians refer to it as the *"kill-the Internet power"* because of the arbitrary nature of this regulation (Keane, 2012b). When it comes to the Internet shutdown episodes, I will provide a recount of the facts in the next paragraphs.

On September 3, 2009, for one hour, from 7:50 to 8:50 a.m. Telstra international Internet network went down (N. Farrell, 2009; Robinson, 2009). Telstra called it an accident despite questioning of some members of the civil society. The same episode and justifications occurred in 2012 and 2016 (Danckert, 2016; Kidman & Allen, 2012) (See figure 08). It is important to note that Telstra, a former government-owned ISP, controls 90% of the Internet subscribers; the remaining ISPs (the ones that control the 10%) depend entirely on Telstra. Therefore, if Telstra is down, most of the Internet service in Australia will be down (Hernandez, 2014).

Figure 08.- Timeline Australian Internet Shut Downs (2009-2016)



Despite all these instances, it is also important to point out that in 2011, after the Egyptian shutdown, Steven Conroy (as I mentioned, the former Australian Communications Minister) denied the use of similar policies in Australia under any circumstances (LeMay, 2011; Tuutti, 2011). Nevertheless, at the same time, Mr. Conroy argued that the Internet cannot be a space wholly unregulated and that the government does not trust in the Australian ISPs (LeMay, 2010a).

Legally speaking, about the government's capacity to control the Internet infrastructure, academics refer to the provision 581 of the Telecommunications Act of 1997. According to the statute, the authority to act over the Internet infrastructure would be the Australian Communications and Media Authority (ACMA) and the Attorney General.

Telecommunications Act of 1997.-

…

Part 34—Special provisions relating to functions and powers of the ACMA and the Attorney General in respect of telecommunications

…

581 Power to give directions to carriers and service providers

(1) The ACMA may give written directions to:

(a)a carrier; or

(b)a service provider;

in connection with performing any of the ACMA's telecommunications functions or exercising any of the ACMA's telecommunications powers.

(2) This section is not limited by any other provision of a law that:

(a)confers a function or power on the ACMA; or

(b)prescribes the mode in which the ACMA is to perform a function or exercise a power; or

(c)prescribes conditions or restrictions which must be observed in relation to the performance by the ACMA of a function or the exercise by the ACMA of a power.

(3) If:

(a)a person who is a carrier or carriage service provider proposes to use, or uses, for the person's own requirements or benefit, or proposes to supply, or supplies, to another person, one or more carriage services; and

(b)the Attorney-General, after consulting the Prime Minister and the Minister administering this Act, considers that the proposed use or supply would be, or the use or supply is, as the case may be, prejudicial to security;

the Attorney-General may give to the carrier or carriage service provider a written direction not to use or supply, or to cease using or supplying, as the case may be, the carriage service, or all of the carriage services.

(3A) A direction under subsection (3) must relate to a carriage service generally and cannot be expressed to apply to the supply of a carriage service to a particular person, particular persons or a particular class of persons.

(4) A person must comply with a direction given to the person under subsection (1) or (3).

(5) In this section:

> security has the same meaning as in the Australian Security Intelligence Organisation Act 1979.

According to the text of the telecommunications statute, provision 581 enables the attorney general, after consulting the Prime Minister and the Minister of Telecommunications, to direct a request to any telecommunications carrier or service provider to stop providing service if it is "prejudicial to security". When "something is prejudicial to security," that will be defined by the Australian Security Intelligence Organisation (ASIO). In other words, an administrative authority, ASIO, is the one that will decide what a matter of national security is, and the attorney general will decide if the situation is of so much gravity that shutting down the Internet is an option. This set of legal powers existed since 2003 when the Australian Parliament amended the statute as part of a counter-terrorism measure (Keane, 2012b).

3.6.3. United Kingdom (U.K.)

The United Kingdom of Great Britain and Northern Ireland, commonly known as the United Kingdom (U.K.) or Britain, is a well-consolidated democratic regime and a constitutional monarchy with a parliamentary system. It is also the progenitor of the common law system. The U.K. is one of the five permanent members of the United Nations Security Council (UN, 2014b) and a member of the OECD (OECD, 2014). From an economic point of view, the U.K. is the sixth-largest economy in the world and the third-largest in Europe after Germany and France (IMF, 2014).

In the past, the U.K. was involved in multiple acts of government control over the Internet. In the mid-1990s the U.K. (alongside with Germany and France) focused on self-regulation of

content. However, this was difficult to control. In March 1996, the British Trade and Industry Minister claimed that the government should encourage ISPs to “voluntarily control” the content they provided to the end-users (Sorensen, 1996).

In 2001, the U.K. government threatened to prosecute under criminal charges to ISPs for distributing illegal adoption sites. As a consequence, by 2005 the U.K. government enacted laws that require ISPs to remove content that was considered inappropriate or unlawful (Subramanian, 2011).

In 2010, the British government wanted to impose limitations over the ISPs to provide pornography on an 'opt-in' basis. The same year the government ordered the ISPs to block access to a file-sharing website Newzbin2 (Mennecke, 2010). In 2016, the British Parliament passed one of the most controversial bills banning encryption (Lomas, 2016). Despite having these strict policies, back in 2011, the U.K. government was highly critical of the Egyptian Internet shut down (Clegg, 2011).

In 2011, between August 6 and 11, during the riots in London, an episode known as “BlackBerry riots,” the British Prime Minister at the time, David Cameron, made public his desire to have a “kill switch” for social networks platforms (Cameron, 2011b). Mr. Cameron blamed social networks for helping to organize criminal actions during the riots in ways the police was not able to control (Cameron, 2011b). However, what is not very well known is that previously Mr. Cameron considered shutting down the Internet (Ghosh, 2011; Marsden, 2011).

Nevertheless, the Foreign Secretary William Hague persuaded Mr. Cameron against the use of this extreme policy because shutting down the Internet would lead to accusations of hypocrisy over the rights of free speech in the U.K. In consequence, the British government abandoned the plan of shutting down the Internet after possible comparisons with the Arab spring

(with the Egyptian case in particular that happened the same year) and restrictions over the freedom of speech as they happen in China (DH, 2011; Ghosh, 2011; Williams, 2011). The British parliament never discussed a bill granting legal powers to the British government to shut down the Internet.

After the debate in London about shutting down the Internet and the BART episode in the U.S., the Chinese news service Xinhua reminded that in a speech delivered in Kuwait in February, the British prime minister argued that freedom of expression should be respected the same "in Tahrir Square as much as Trafalgar Square" (Xinhua, 2011, para.5). They accused the U.K. government of hypocrisy and also claimed that the Chinese government "may wonder why western leaders, on the one hand, tend to indiscriminately accuse other nations of monitoring, but on the other take for granted their steps to monitor and control the Internet" (Xinhua, 2011, para.9).

Besides the U.K. government, the academic sector also discussed the subject. According to some academics, such as David Eagleman, author of "Why the Net Matters," Section 132 of the Communications Act of 2003 (See Appendix 2) grants special powers to the "Independent regulator and competition authority for the United Kingdom communications industries," known as OFCOM. According to section 132, OFCOM can request to any U.K.-based ISP the suspension of the service to preserve the "public order" or in case of a massive cyberattack. This legislation is part of the national security strategy of the U.K. (Harding, 2011; Marsden, 2011).

OFCOM has the legal authority to act on behalf of one of the ministers, most likely the minister of culture, who would be the one who has legal power to shut down the Internet (Harding, 2011; Marsden, 2011). Along with section 132 of the Communications Act, the part 2 of the Civil Contingencies Act of 2004 also would give to the executive branch legal authority to request to the ISPs the suspension of the Internet service. According to part 2 of the Civil Contingencies Act,

the executive branch is entitled to create emergency regulations if the U.K. faces a national security threat.

> "Civil Contingency Act 2004"
> "Part 2 Emergency powers
> 19 Meaning of "emergency"
> "(1) In this Part "emergency" means—
> (a) an event or situation which threatens serious damage to human welfare in the United Kingdom or in a Part or region,
> (b) an event or situation which threatens serious damage to the environment of the United Kingdom or of a Part or region, or
> (c) war, or terrorism, which threatens serious damage to the security of the United Kingdom."
> (…)"
> "(6) The event or situation mentioned in subsection (1) may occur or be inside or outside the United Kingdom.
> 20 Power to make emergency regulations
> (1) Her Majesty may by Order in Council make emergency regulations if satisfied that the conditions in section 21 are satisfied.
> (2) A senior Minister of the Crown may make emergency regulations if satisfied—
> (a) that the conditions in section 21 are satisfied, and
> (b) that it would not be possible, without serious delay, to arrange for an Order in Council under subsection (1).

According to the representatives of the Department for Culture, Media and Sport, a government order to shut down the Internet has to follow a grave threat, like a significant cyberattack (Harding, 2011). Although an interested party may challenge the government's request in an urgent judicial review, a threat to the public order or a national security emergency is unlikely to be overturned, and therefore all operators of telecom infrastructure must follow the government request (C. Russell, 2011). Differently, from the opinion of this department, an academic sector considers that, despite the powers contained in section 132, the only thing the U.K. government can do is to serve the ISPs with a notification. In the case that one or more ISP refuse the government's request, the punishment is merely a fee (Winder, 2011).

By 2017 the U.K. government identified “cyber” as one the major threats to their national security, in particular when the U.K.’s Internet and critical national infrastructure are involved (POST, 2017). In the same line, the current U.K. administration, led by Theresa May, is taking a more aggressive approach when is about Internet regulation:

“Some people say that it is not for the government to regulate when it comes to technology and the internet, ….We disagree.” (Krieger, 2017, para.4).

3.6.4. United States of America (U.S.)

The U.S. is a federal republic with a presidential system. Until 2016, the U.S. was considered a consolidated democratic regime. In 2017, the EIU re-categorized the U.S. from being a consolidated democracy into a “flawed” one, (or a “young” democracy using the terminology of this dissertation). According to the EIU report, the change occurred because of the erosion of confidence in government and public institutions (EIU, 2017). The U.S. is also an OECD member, and its per capita GDP is one of the highest in the world (IMF, 2014).

The U.S. legislative branch had a prolonged debate to grant legal power to the president to shut down the Internet (CDT, 2009; Phillip Reitinger, Butler, Schwartz, & Chipman, 2011; Lieberman, 2011a). The U.S. Congress did not pass the proposed bills, partially because of the opposition by members in civil society (CDT, 2009; MacKinnon, 2012). However, according to members of the government, the president already has authority to shut down the Internet according to current telecommunications laws (Lieberman, 2011a).

The case of the U.S. demonstrates how national security concerns have been the primary reason to control the telecommunication system since the beginning of the twentieth century.

Section 606 of the Communications Act of 1934[16] contains special powers for the U.S. president in case of war. Conditions included in subsection (a) of section 606 are specific to the preferential communications to be used during wartime (Opderbeck, 2012, 2013):

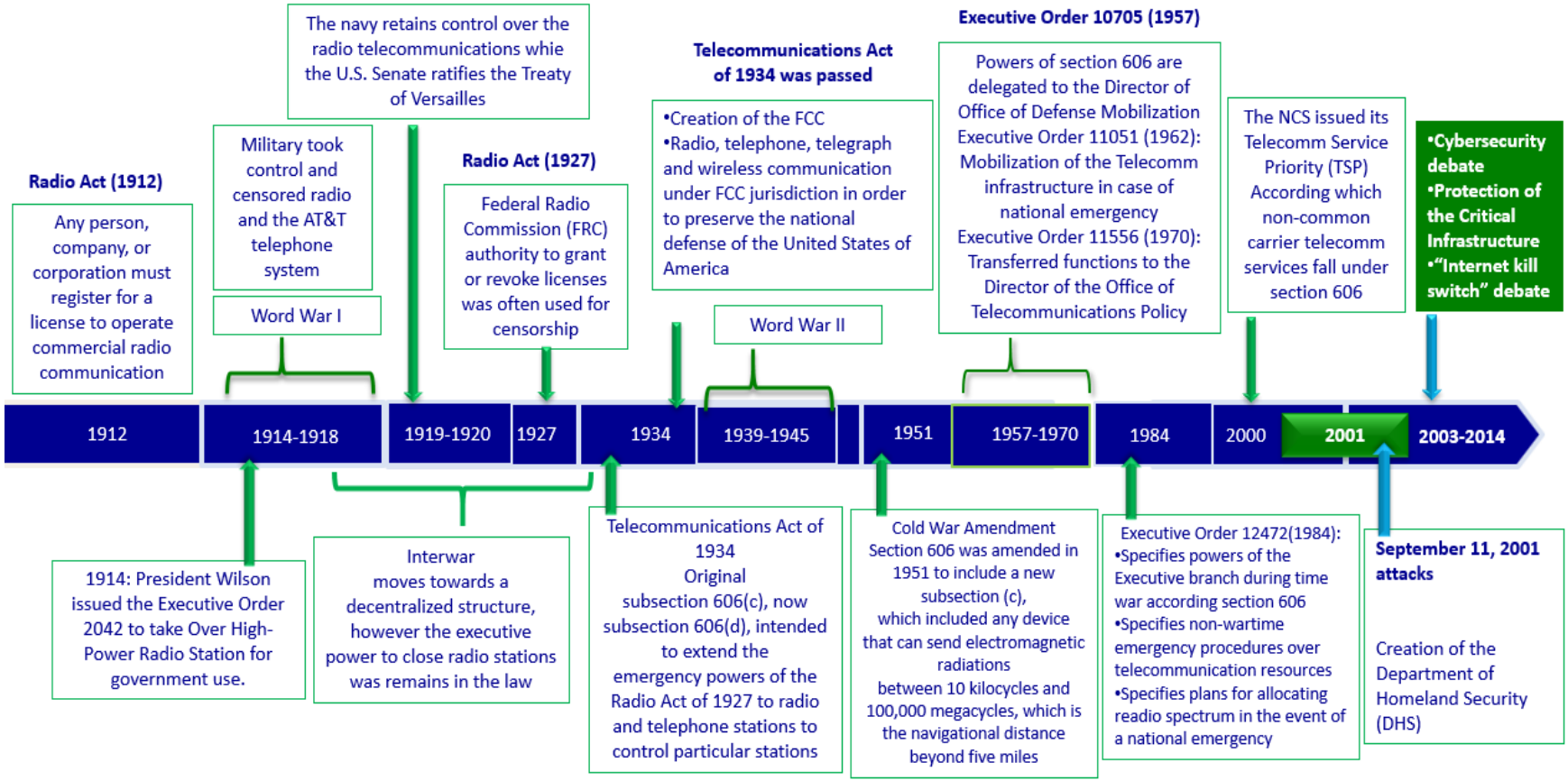
1. During the continuance of a war in which the U.S. is engaged, and
2. If the President considers that prioritized communications are required for the national defense and security.

If these two conditions met, the president is authorized to act according to his or her judgment and to direct the telecommunications system to protect the national security within U.S. territory. (Medows, 2012; Opderbeck, 2012, 2013).

The provisions of section 606 are the result of a long legislative practice of controlling the telecommunications system, long before the Internet (Horvitz, 2013). This legislative practice started during World War I, continued during the interwar period and the World War II, until today. Between 1951 and September 11, 2001, the history of the Presidential directives and executive orders was focused on defense during the Cold War, specifically against nuclear attacks. After September 11, 2001, the focus changed to terrorism and cyberterrorism, consolidating many functions in the Department of Homeland Security (DHS). The content of bills and directives changed, and it turned to include all of what today falls under the label of "cybersecurity" (Acklyn Murray, Zeadally, & Flowers, 2012; Opderbeck, 2012, 2013). I present a timeline where I refer to the most important laws and bills enacted between 1912 and 2001 (please see figure 09 in the next page).

[16] Successor of the Radio Act of 1912

Figure 09- U.S. Government Control over the Telecommunications Infrastructure



Between 2009 and 2012, the U.S. Senate was the center of debate for several bills that attempted to give to the President legal power to shut down the Internet and take over the Internet communications of any public or private entity (P. M. Shane, 2012; Thompson, 2012). None of these bills passed because of the strong opposition by civil society organizations, which were mostly concerned about two specific problems that were common to the bills' drafts (MacKinnon, 2012; Medows, 2012; Opderbeck, 2013):

1. The potential impact on freedom of speech

   Over the same packets, wires, and routers that form the Internet, travels information about the U.S. critical infrastructure and people's communications. Therefore, any action to protect the critical infrastructure will affect the communication process. In this way, an operation of governmental control would have a direct impact on civil liberties, such as the freedom of speech, one of the cornerstones of a democratic system.

2. Limits of the President's authority

   The text of the bills never clarified the extent of the president's authority. Additionally, some scholars and government agencies representatives consider that the president already has authority to shut down the Internet according to the Executive legal powers of the Telecommunications Act of 1934.

In the next paragraphs I will provide an overview of the bills proposed within the U.S. Senate between 2009 and 2011.

On April 1, 2009, Senator Rockefeller presented bill S.773 to the Committee on Commerce, Science, and Transportation; from that moment, the bill became officially known as the "Cybersecurity Act of 2010". The goal of S.773 was strengthening the security of the information infrastructure within the U.S. territory by "increasing the information security

workforce, creating new authorities for the federal government, and promoting public-private collaboration" (U.S. Senate, 2010a).

The cybersecurity act of 2010 distinguished the character of public-private relationships to protect cyberspace (U.S. Senate, 2010a). Section 18 paragraphs 2 and 6 of S.773 attempted to give the President legal authority to shut down the Internet within U.S. territory:

> "S.773.- Cybersecurity Act of 2009"
> Sec. 18. Cybersecurity responsibilities and authorities.
> "The President— "
> ….
>
> "(2) may declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network;"
> …
> "(6) may order the disconnection of any Federal Government or United States critical infrastructure information systems or networks in the interest of national security;"

For this reason, bill S.773 was very unpopular among civil society organizations. The main points of critique were that the bill did not provide any guidance or limits to the powers of the president and that it did not make distinctions between the elements of the communications infrastructure that supports free speech and those that do not (CDT, 2009). For this reason, digital activists baptized S.773 as the *"Internet kill switch"* bill.

Before reporting S.773 to the Senate on December 22, 2010, sponsors of the bill removed section 18. Despite this modification, the U.S. Senate didn't approve bill S.773 (U.S. Senate, 2010a).

On May 29, 2009, President Obama declared the digital infrastructure (the Internet included) as a "strategic national asset" to be protected by the U.S. government and private companies because digital technologies are vital for the prosperity of the U.S. national economy during the 21st century (White House, 2009). Following the White House policy, on June 6, 2010,

Senator John Lieberman (D) introduced bill S.3480, titled “Protecting Cyberspace as a National Asset Act of 2010,” also known as PCNAA. The main purpose of bill S.3480 was to amend the Homeland Security Act of 2002 and related laws by improving “the security and resiliency of the cyber and communications infrastructure of the United States”. Unlike its predecessor, bill S.773, S.3480 was an outcome of the Committee on Homeland Security and Governmental Affairs (Lieberman, 2010).

Senator Lieberman remarked that the Internet is constantly under attack; therefore, the purpose of bill S.3480 was to secure the most “critical cyber networks” and to be prepared for potential cyberwarfare and cyberattacks. As it happened with bill S.773, sponsors of bill S.3480 also expected to strengthen the collaboration between the public and private sectors to protect the critical infrastructure. Nevertheless, S.3480 even attempted to give to the president legal power to “impose emergency measures on a select group of the most critical infrastructure” to preserve it (U.S. Senate et al., 2010). If approved, S.3480 would have granted to the president the capacity to declare a national cyber emergency that eventually could force owners and operators of critical infrastructure into immediate compliance with any emergency measure or action, including shutting down the Internet (Thompson, 2012).

The possibility of shutting down the Internet was not included in S.3480 as it was in bill S.773, but it was not rejected either.

> “S.3480.- Protecting Cyberspace as a National Asset Act of 2010”
> Sec. 249. National Cyber Emergencies
> …
> ‘‘(c) COMPLIANCE WITH EMERGENCY MEASURES. —
> ‘‘(1) IN GENERAL. —Subject to paragraph (2), the owner or operator of covered critical infrastructure shall immediately comply with any emergency measure or action developed by the Director under this section during the pendency of any declaration by the President under subsection (a)(1) or an extension under subsection (b)(2).

Just like in the case of the previous bill (S.773), bill 3480 was also baptized as the "Internet kill switch" bill, and many civil society organizations opposed it (MacKinnon, 2012). Alongside the potential attributions of the president, according to the text of S.3480, owners or operators of the covered critical infrastructure (CCI), will have to comply with any emergency measure established by the Department of Homeland Security (U.S. Senate et al., 2010). Sponsors of bill S.3480 never clarified the concept of "emergency measures". Those words could mean anything, even shutting down the Internet (Theohary & Rollins, 2011)

On the other hand, despite so much criticism, it also must be clear that Senator Lieberman and co-sponsors of S.3480 always denied that their intention was granting to the president attributions to shut down the Internet within U.S. territory (Lawson, 2011).

On December 15, 2010, Senator Lieberman presented the report 111-368 about bill S.3480 within the Committee on Homeland Security and Governmental Affairs (U.S. Senate, 2010b). The Committee then placed S.3480 on the Senate legislative calendar under General Orders Calendar No. 698, but the bill was not approved (Lieberman, 2010).

It is also important to note that, previously, on June 16, 2010, Representative Jane Harman (D) had introduced Bill H.R.5548 within the House of Representatives. The full text and title of H.R.5548 were identical to the version of S.3480. H.R. 5548 was referred to multiple sub-committees, but it was never enacted (Govtrack.us, 2010; Harman, 2010).

Finally, on February 17, 2011, again under the sponsorship of Senator Joseph Lieberman and having as co-sponsors Senators Collins (R) and Carper (D), bill S.413 was introduced in the U.S. Congress. Just as it happened with its predecessor (S.3480), sponsors submit S.413 to the Committee on Homeland Security and Governmental Affairs.

Bill S.413 was titled ‘‘Cybersecurity and Internet Freedom Act of 2011,’’ also known as CIFA (Lieberman, 2011b). The official purpose of bill S.413 was (like bill S.3480) to amend the Homeland Security Act of 2002 and related laws to improve the security and resiliency of the communications infrastructure in the U.S., especially the Internet. The purpose of S.413, similar to its predecessors, was also to address the growing threat of attacks against the U.S. critical infrastructure (Lieberman, 2011).

Unlike its predecessors, bill S.413 acknowledges the fact that shutting down the Internet is not possible in the U.S. territory because of the high level of Internet penetration rate and because the existence of thousands of ISPs makes this technically impossible[17].

At the same time, S.413 ensured that “the President cannot take any action that would limit free speech or shut down the internet (Lieberman, 2011a). Therefore, unlike its two predecessors, bill S.413 declares that neither the President nor any other federal employee has authority to shut down the Internet:

> “S.413.- Cyber-security and Internet Freedom Act of 2011”
> “Sec. 2. Internet Freedom Act.”
> “(…)
> (b)FINDINGS.—Congress finds that—
> (…) (10) neither the President, the Director of the National Center for Cyber-security and Communications, nor any other officer or employee of the Federal Government should have the authority to shut down the Internet.”

During the introduction of S.413 within the U.S. Senate, Senator Carper underlined that S.413 contained explicit provisions to prevent the president from applying any restrictions over

[17] “S.413.- Cyber-security and Internet Freedom Act of 2011”
“Sec. 2. Internet Freedom Act.”
“(…)
(b) FINDINGS.—Congress finds that—
(…) (4) the Internet has developed into a robust network within the United States, with thousands of providers, making it technically impossible to shut down the Internet;”

Internet traffic. Additionally, Senator Lieberman also stated that bill S.413 only would clarify the president's authority to act in the event of a cyber-attack (Lieberman, 2011a). However, on this matter, Senator Lieberman also stated that the executive branch believes that, according to the telecommunications law from 1934 and further amendments of 1996, the president already has the faculty to disconnect some parts of the Internet (Lieberman, 2011).

As part of the debate within the U.S. government, officials from DHS consider that section 706 of the Telecommunications Act gives attributions to the president to take extraordinary measures to respond to a cyberattack (Lieberman et all, 2011b). On the other hand, within the U.S. Senate, some senators have recognized that the war powers of the president, as the telecom statute establishes, are broad and vague, so much that "in the event of a cyber-attack, the President's authorities are broad and ambiguous—a recipe for encroachments on privacy and civil liberties." (Senator Collins, 2011, p.912).

On May 23rd, 2011, the Committee on Homeland Security and Governmental Affairs conducted hearings about bill S.413; however, the U.S. Senate never passed S.413.

In parallel to the Senate debate, on May 12, 2011, the Obama Administration prepared a set of recommendations for new cybersecurity legislation. One of the proposals was related to a "Cybersecurity Regulatory Framework for Covered Critical Infrastructure" (Schmidt, 2011). I will call this document the White House proposal of 2011.

On May 23, 2011, a hearing was conducted within the Committee on Homeland Security and Governmental Affairs of the U.S. Senate to assess the White House proposal (US Senate, 2011). Both projects, S.413 and the White House initiative, agree that DHS would have the authority to identify and decide what cyber infrastructures and critical infrastructures are, whether they belong to the private or public sector, and act over them in the eventual case of a cyberattack.

Like the Senate bills, the White House proposal also incorporated provisions to include the private sector within the national security strategy (Schmidt, 2011).

The White House Proposal is broadly like the previous bills under study. About the possibility of shutting down the Internet and why the White House proposal does not contain any changes to the president's powers provided in the telecommunications law of 1934, on May 23, 2011, the Committee on Homeland Security and Governmental affairs within the U.S. Senate conducted a hearing. In that session, Philip Reitinger (at the time, the deputy undersecretary for the National Protection and Programs Directorate, from DHS), stated that the White House proposal contains the same attributions for the president established in the telecommunications act of 1934 (Phillip Reitinger et al., 2011).

Nevertheless, Mr. Reitinger also stated that, because national security situations are "context-driven," any final response about how to act requires further discussion and debate among all the stakeholders involved (Philip Reitinger, Butler, Schwartz, & Chipman, 2011). Finally, Mr. Reitinger acknowledged that the president will use the authority conferred by law in the "right way". However, he did not provide any further explanation about what the "right way" means (US Senate, 2011).

On this matter, the essential difference between the White House initiative and bill S.413 is that the White House proposal did not contain specific emergency powers as bill S.413. The reason for this lack of emergency powers would lie in the fact that the current administration considers that the president already has authority to shut down the Internet, according to the Telecommunication Act of 1934 (Medows, 2012).

Figures 10, 11 and 12 shows a timeline of the introduction of the bills, the variation in the content of the different U.S. Senate bills and the White House initiative.

Figure 10.- U.S. Congress Internet Shutdown Bills– Timeline

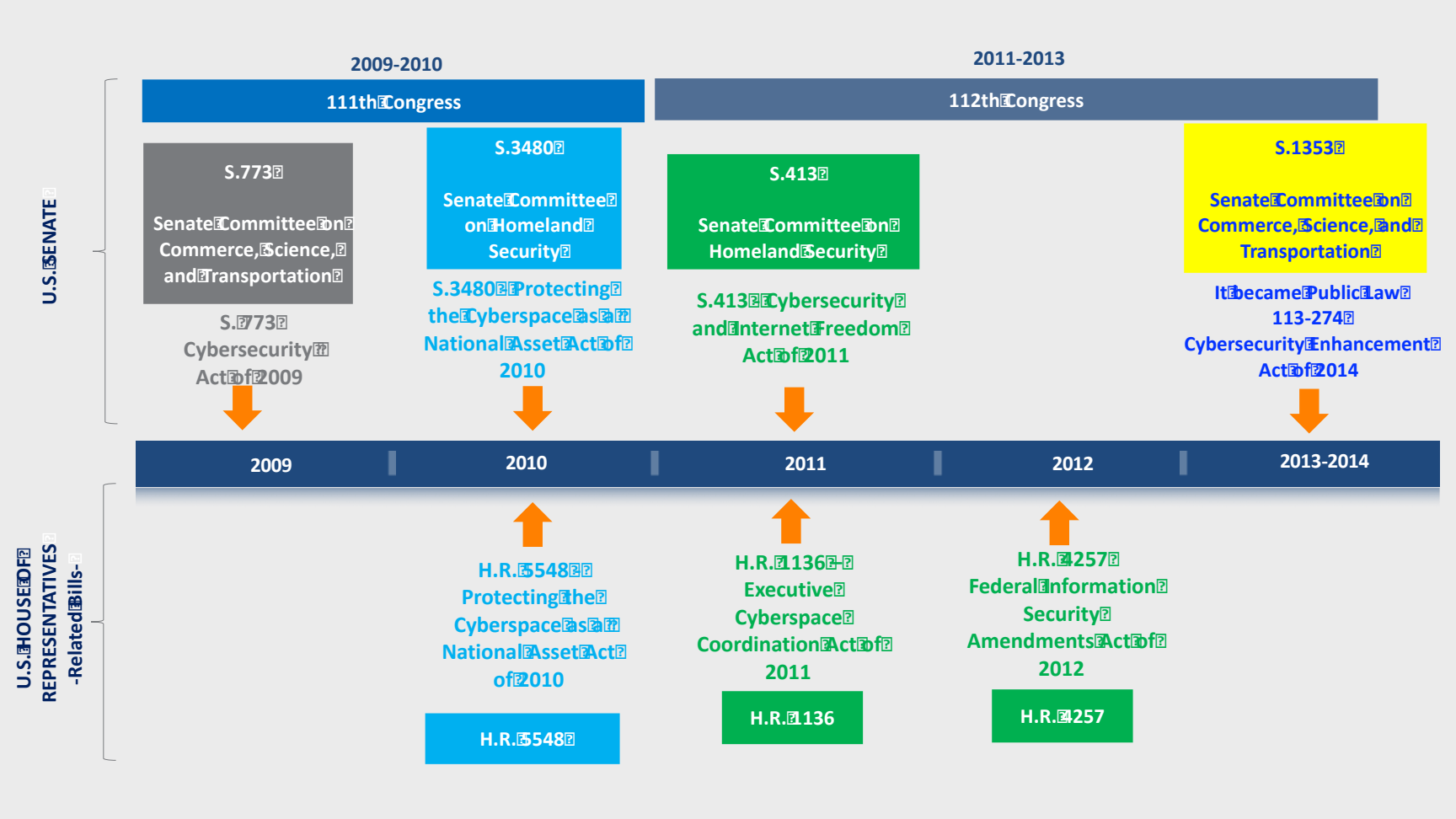


Figure 11.- U.S. Congress Internet Shutdown Bills– Specific Provisions about Internet Shutdowns

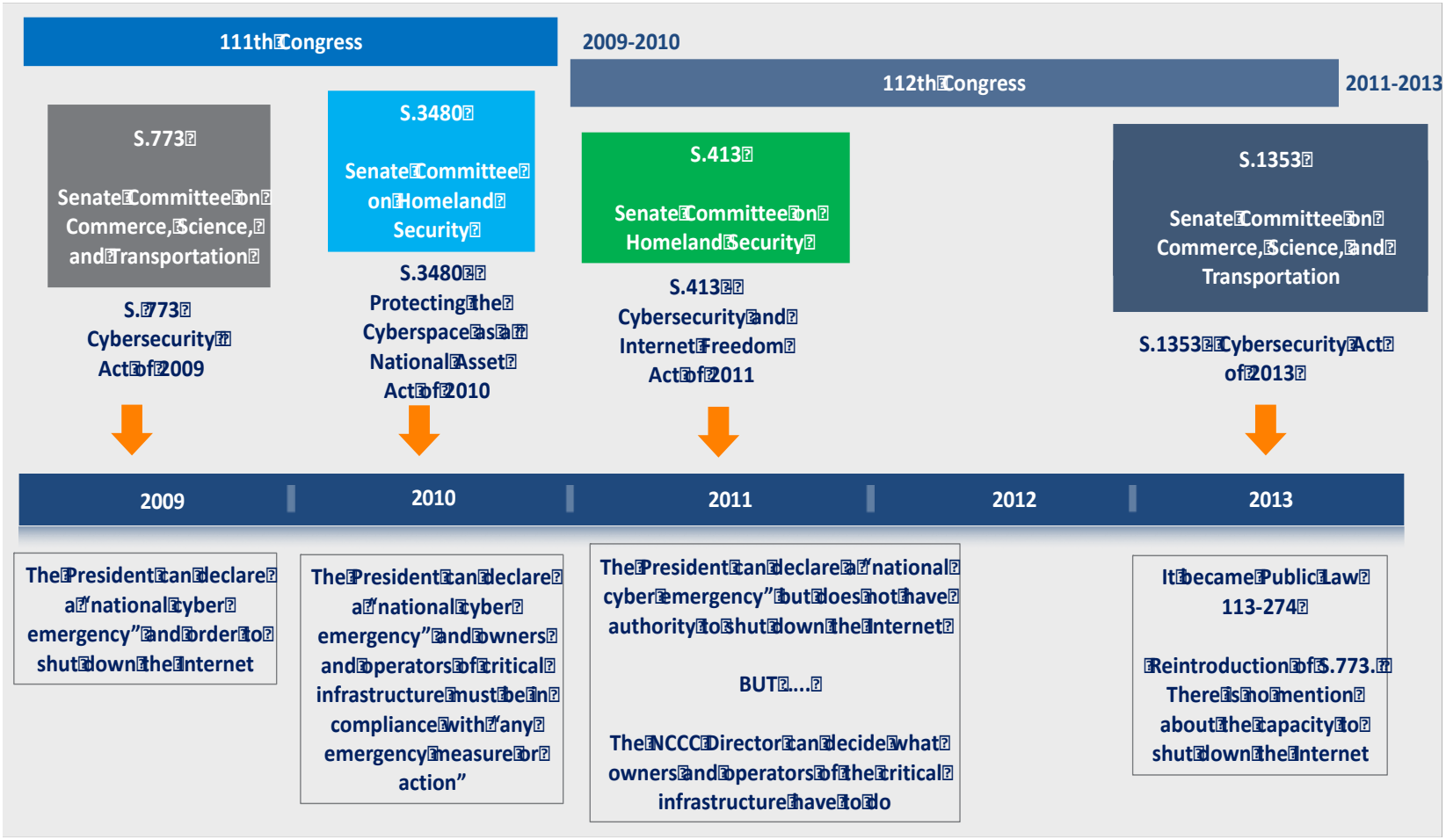
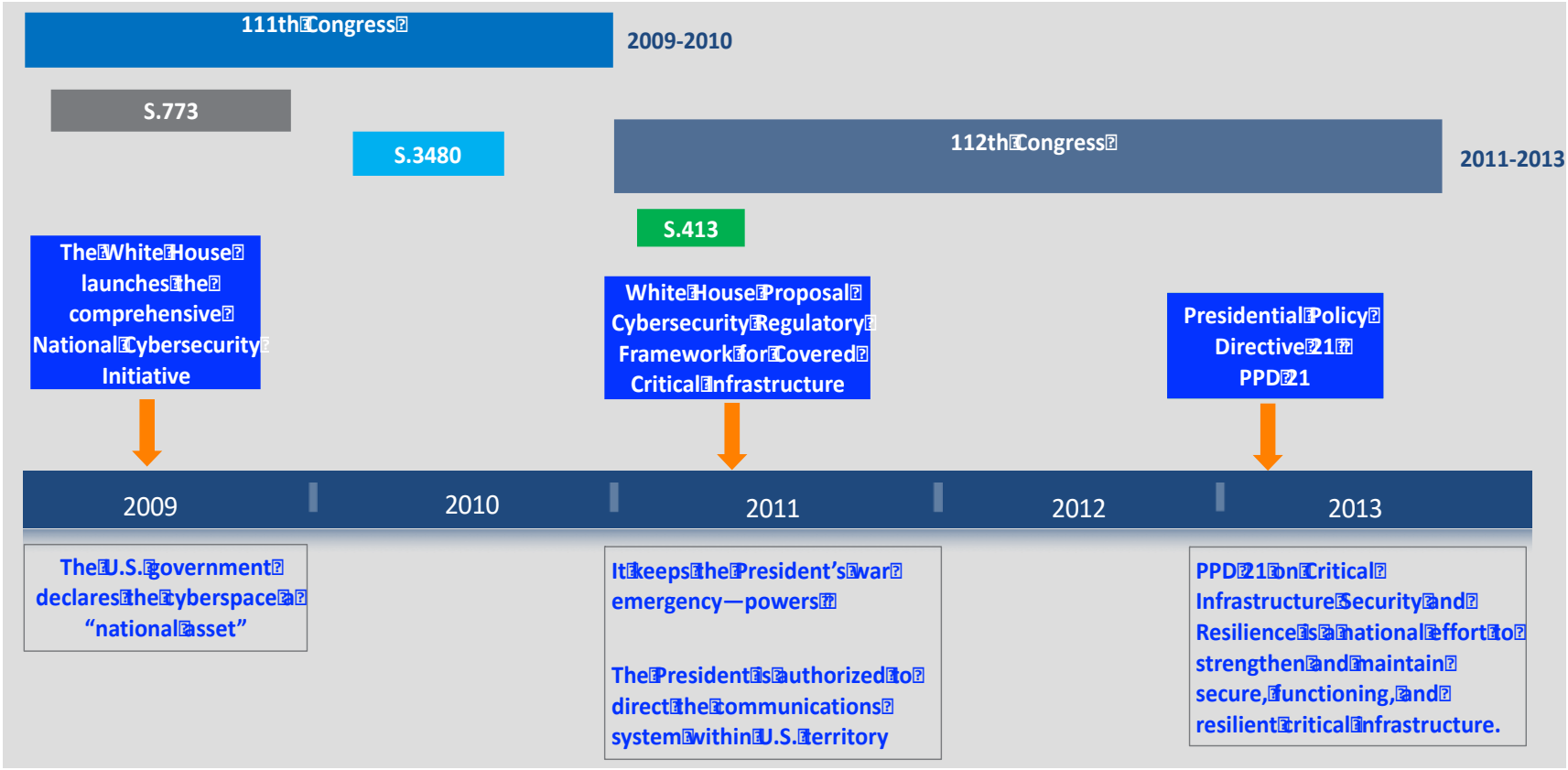


Figure 12.- U.S. White House Proposals Internet Shutdown Related



Finally, in the case of the U.S., it is important to refer to an aspect not related to any type of academic or legal debate. In the next paragraphs, I will provide details about a controversial protocol whose content is unknown. On July 3, 2011, a BART (Bay Area Rapid Transit) police officer shot and killed a homeless man in the Civic Center station in San Francisco. Following this event, protestors congregated in BART stations, opposing what they considered to be an inappropriate response to a suspected mentally ill man. Following protests, the regular communication BART service got disrupted. To prevent future protests, and without prior notice, BART shut down wireless communications service underground for three hours. The disruption prevented protesters from any communication. This government action was justified in the name of public security (Elinson, 2011; Elinson & Walter, 2011).

After the 2005 London underground bombings, U.S. authorities believed that terrorists could detonate a similar bomb through the wireless networks in New York City. With this fear in mind, the President's National Security Telecommunications Advisory Committee commissioned a task force to create a mechanism for coordinating government and industry actors' actions to implement emergency wireless network shutdowns. The result of this commission was the "Standard Operational Protocol 303 Emergency Wireless Protocols," (SOP 303).

Following the BART incident, the Electronic Privacy Information Center (EPIC) became interested in SOP 303. In 2012, EPIC filed a FOIA[18] request and sent to DHS questions about SOP 303 implementation, and any related guidelines or protocols (EPIC, 2012). DHS responded to the request by turning a crossed-out-document where the only words to read were "SOP 303" (Brownlee, 2015; DeSoto, 2015). Following the analysis of the document, EPIC and public interest

[18] The Freedom of Information Act (FOIA) is a law that gives U.S. citizens the right to access information from the federal government. The procedure to access information under the rules of the freedom of information act is known as a "FOIA request".

advocacy groups, baptized SOP 303 as the U.S. protocol to shut down the Internet or the "cellphone kill switch" (EPIC, 2011; Jacobs, 2013; Kravets, 2015b; NSTAC, 2006).

Facing these circumstances, on February 27, 2013, EPIC filed another FOIA request for the protocol (Clabough, 2015; Ditz, 2015). It was in that moment that, official documents disclosed in the Court described SOP 303 as an emergency wireless protocol, which purpose is "codifying a shutdown and restoration process for use by commercial and private wireless networks during national crises" (Whittaker, 2013, para.4). The DHS argued that they couldn't disclose this protocol for reasons of national security, and initially the judicial branch ruled against the DHS arguments. The DC District Court ruled that exemptions contained in the FOIA regulations don't apply to this case (DeSoto, 2015). The DHS appealed, and in February 2015, the DC Court of Appeals reversed the District Court's judgment (Kravets, 2015a, 2016; United States Court of Appeals, 2015).

In this scenario, as far as we know, the purpose of SOP 303 is preventing terrorists to activate bombs through wireless networks. The government would be explicitly authorized to target a "localized area," whether it is a bridge, a building or a metropolitan area (Kravets, 2015b). However, after the BART episode, it became a question whether SOP 303 also would be used to prevent peaceful protestors. Another issue that came up was whether cellphone and Internet access are part of the First Amendment right and should not be taken away in national emergencies. On January 11, 2016, the U.S. Supreme Court declined to review EPIC v. DHS (Shin, 2015). Despite the gravity of the implications of SOP 303 capabilities, nothing else is known about it.

3.6.5. República Bolivariana de Venezuela (Venezuela)

Venezuela is a republic with a federal presidential system. Venezuela is considered a hybrid regime because of the permanency in power of the same party since 1999, continuous violations over the freedom of speech, and because members of rival political parties formally contested the last elections in 2013. Additionally, since 2014, several political rivals to the current regime have been imprisoned, and their situation remains uncertain (Brodzinsky, 2015; EIU, 2011, 2017; theguardian, 2017; Villafranca, 2013). In May 2017, the current Venezuelan President, Nicolás Maduro, called to hold elections for a "Constituent Assembly." The purpose of this assembly is to write a new Venezuelan Constitution. Nicolás Maduro has disowned the authority of the current Venezuelan Congress, where his party does not have majority. When asked about the necessity to call for these new elections, Maduro answered that he needs to "transform that rotten National assembly," referring to the current Venezuelan Congress (Ore & Chinea, 2017, para.9). On July 30, 2017, when the elections took place, Caracas (the capital city) was full of protests, and government forces killed at least ten protestors (BBC Mundo, 2017).

Despite having numerous oil reserves, the Venezuelan economy is in crisis and is considered one of the most corrupt and dangerous places in the world. In early 2013, Venezuela devalued its currency due to growing shortages in the nation-state, and the economy fell into recession. Alongside with the economic crisis, since late January 2014, Venezuela lives in turmoil because of the national protests that demand democratic changes in the government (EFE, 2015, 2017; Naim & Toro, 2016; Pardo, 2016).

To avoid the U.S. led financial sanctions, Nicolás Maduro looked for alternatives into the digital currency, and he announced the creation of the "petro," a crypto currency backed by oil reserves (Ulmer & Buitrago, 2017). The Venezuelan government has introduced "petro",

abbreviated as “PTR,” as the realization of president Hugo Chavez’s idea of “a strong currency backed by raw materials.” (Greenfield, 2018, para.4).

In terms of control over the Internet infrastructure, Venezuela shut down the Internet three times (See figure 13): (1) the first Internet shutdown took place during the time of the national presidential elections in 2013 (See figure 13), (2) the second Internet shutdown occurred during the nationwide protests in 2014 (and was concentrated in San Cristóbal, the capital city of Táchira, located at the border with Colombia) (Diaz Hernandez, 2013; Mora, 2014) and 3) at the beginning of 2015 the Internet went down again. During the last Internet shutdown, the government claimed an accident because the government-owned CANTV, the leading Internet service provider that handles almost entirely the number of Internet subscribers in Venezuela, had technical problems providing the service (El Universal, 2015; Gomez, 2013).

Figure 13.- Internet Shut Down Venezuela, 2013 Presidential Elections

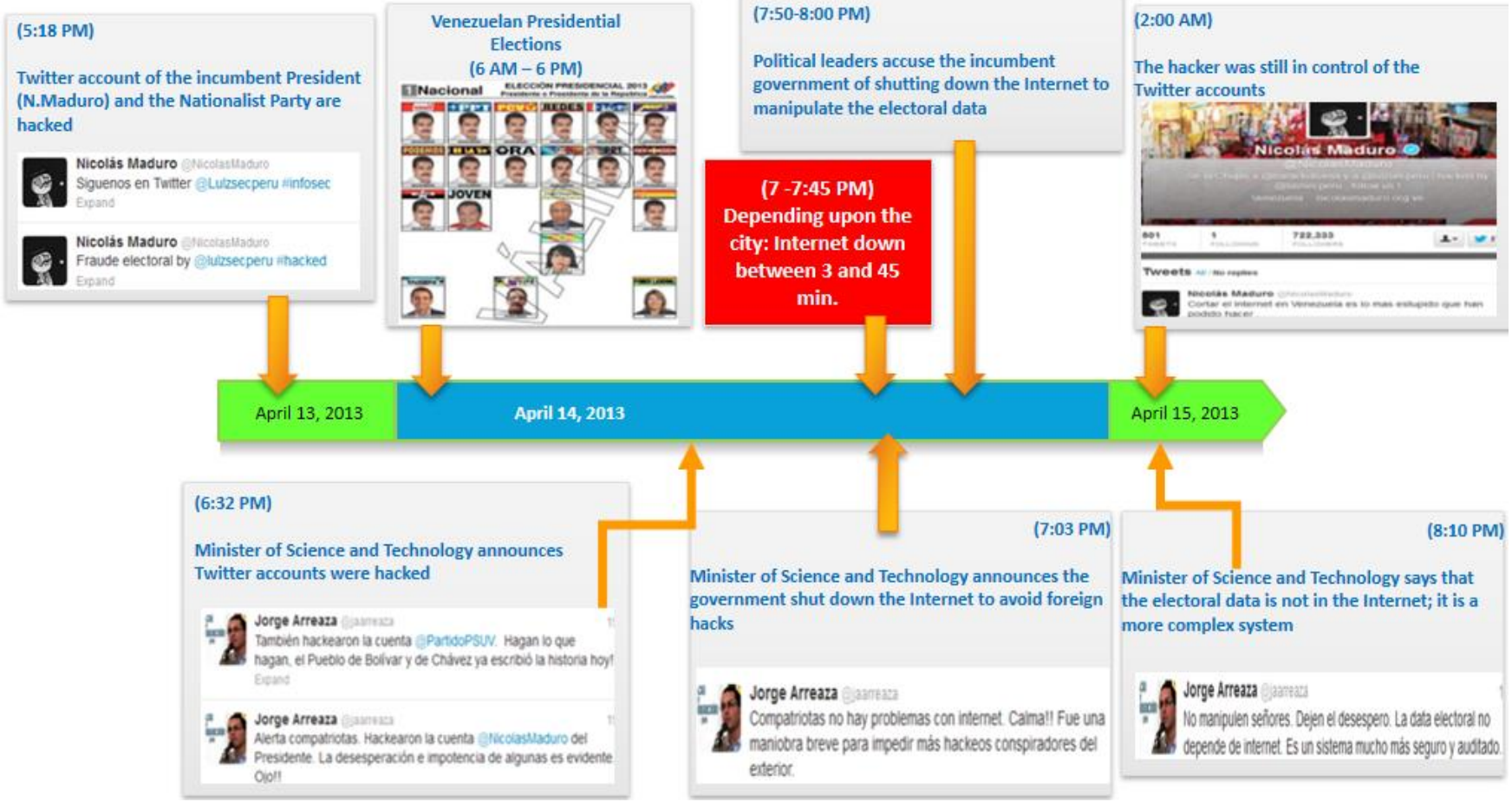


Figure 14.- Venezuela Internet Shutdowns Timeline

Venezuela has 23 internationally connected domestic providers, and these periodic Internet shutdowns are not considered of the same magnitude as the Egyptian one. Venezuela suffered short-term-episodes of Internet shutdown, differently from the national five-day-Egyptian case. Additionally CANTV, the biggest government-owned-ISP has experienced loss of transit through international providers through the years (Dyn, 2014b).

In 2000, and according to the provisions of the National Statute of Telecommunications, the Venezuela government started drafting a law titled "Responsabilidad Social en Radio, Televisión y Medios Electrónicos" Act ("Law of Social Responsibility in Radio, Television and Electronic media"), also known as RESORTE law. The purpose of this new law was, according the text of the law itself, strengthening the democratic system and to encourage the creation of culture of respect towards human rights (Finol & Espinoza, 2015). In article 1 RESORTE emphasizes the duties of the actors considered relevant for the Venezuelan government:

> "Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos
>
> Articulo 1.- Esta Ley tiene por objeto establecer, en la difusión y recepción de mensajes, la responsabilidad social de los prestadores de los servicios de radio y televisión, proveedores de medios electrónicos, los anunciantes, los productores y productoras nacionales independientes y los usuarios y usuarias, para fomentar el equilibrio democrático entre sus deberes, derechos e intereses a los fines de

> promover la justicia social y de contribuir con la formación de la ciudadanía, la democracia, la paz, los derechos humanos, la cultura, la educación, la salud y el desarrollo social y económico de la Nación, de conformidad con las normas y principios constitucionales de la legislación para la protección integral de los niños, niñas y adolescentes, la cultura, la educación, la seguridad social, la libre competencia y la Ley Orgánica de Telecomunicaciones …" (Asamblea Nacional de la Republica Bolivariana de Venezuela, p.1, 2004)

Translation:

Law of Social Responsibility in Radio, Television and Electronic media

> Article 1.- The purpose of this Law is to establish, when is about the dissemination and receipt of messages, the social responsibility for providers of radio and television services, media providers producers, advertisers, independent national producers and users, to promote a democratic balance between their duties, rights and interests for the purpose of promoting social justice and contributing to the formation of citizenship, democracy, peace, human rights, culture, education, health and the social and economic development of the nation, according to the constitutional norms and provisions of the legislation for integral protection of children, culture education, social security and the National Telecom Statute …..

Initially, the law only covered radio and television, but in 2005 an amendment included the Internet. This statute is one of the most controversial rules approved by the Venezuelan Congress because its purpose is to control the content of what is published on the Internet and the rest of the media. RESORTE forbids material considered "offensive," "violent," "disrupt public order," "disown pubic authorities," and "induce homicide." RESORTE also makes third parties, website platforms (such as Twitter and Facebook), responsible for the content posted by Internet users. It is of course for the government authority, the regulator, in this case, to decide when the speech falls into the previous categories (Finol & Espinoza, 2015; Gonzalo, 2010). RESORTE is the final product of years of efforts by former President Hugo Chavez, who vouched to regulate the Internet when he was alive (drupy2000, 2010; El Pais, 2010).

On May 13, 2007, the Venezuelan government enacted the Presidential Decree 2849. The decree 2849 declared a "State of Emergency," in the entire Venezuelan territory for sixty days.

Among the provisions of 2849, the government included the possibility of filtering and surveillance of Internet content. The Venezuelan government justification was the existence of local and international actors interfering in the national economy through the use of the ICT and the cyberspace to promote the hate speech and to create distortion in the Venezuela economy (ISOC, 2017a).

During the first quarter of 2017, the Venezuelan government blocked the sites "DolarToday" and "Maduradas," and attacked at least 11 independent portals and NGOs sites. After March 28, 2017, when Maduro tried to strip Congress from power, the regulator "Comisión Nacional de Telecomunicaciones" (CONATEL) ("National Telecommunications Commission") authorized the censorship of digital TVs Vivo Play, VPI Tv and the Capitolio portal TV channel. It is common to censor websites in Venezuela, to impose restrictions on social networking platforms and to decrease download speed of the Internet services. These are standard practices during times of national unrest. Sites more common to censor are related to the parallel dollar market, media and critics towards the Venezuelan government and former President Chavez (IPYS, 2017).

On June 1, 2017, the President of CONATEL, Mr. Andrés Eloy Méndez, announced that the government was preparing an administrative regulation that would oversee different aspects of the Internet. Some of those aspects include the creation of email accounts, the use of IP addresses and the identification of the author of an action (positive or negative) (Angarita, 2017; El Nacional, 2017). Mr. Méndez was also very clear about how the Venezuelan government would attempt to identify any individual who has an account on a social platform:

> "Estamos evaluando el levantamiento de información de quién abre una cuenta, de quien ejerce un medio electrónico por la plataforma que sea: Twitter, Instagram, Facebook, el que sea" (Angarita, para.3, 2017)

Translation:
"We are evaluating the gathering of information from any person who opens an account, from who uses an electronic medium for any platform, whether it is: Twitter, Instagram, Facebook"

3.6.6. The Republic of Turkey (Turkey)

Turkey is a constitutional republic with a parliamentary system. Turkey is also a member of the Council of Europe, the North Atlantic Treaty Organization (NATO), and the Organisation for Economic Co-operation and Development (OECD) group (Bhalla, 2009; OECD, 2014). Turkey's growing economy and diplomatic initiatives have led to its recognition as a regional power (IMF, 2014).

Turkey is considered a hybrid regime because of its low levels of political participation and government acts over the freedom of speech. The Turkish government has a strong policy to censor Internet content and, since 2007, the court system has been active putting down multiple sites (EIU, 2017; OpenNet, 2013). On May 4, 2007, the Turkish Grand National Assembly (TGNA) passed the Law 5651 titled "Law No. 5651 on Regulating Broadcasting on the Internet and Fighting Against Crimes Committed through Internet Broadcasting," also known as Internet Act (IA) (WIPO, 2008). Law 5651 gave more power to the Turkish regulator (TIB), to (Kizilkaya, 2014; trend, 2014):

1. Block Internet access and censor its content, if a Court approves it within 48 hours
2. Collect Internet traffic information through IP number, subscriber numbers, subscription information form the ISPs, the type of service and the amount of data used

According to the Turkish government, the enactment of law 5651 concerns for the availability of defamatory videos about the founder of the Turkish Republic Mustafa Kemal

Atatürk through YouTube. Additional interests include increasing of child pornographic, and Satanist content on the Internet, information about suicide, or about illegal substances deemed harmful or inappropriate for children. This Turkish law allowed the government to censor websites without even a court order. As consequence of the creation of this new legal statute, until December 2009 there were at least 197 court orders to censor at least 3700 websites (OpenNet, 2013; OSCE RFOM, 2009)

In 2011, thousands of people took the streets and protested against the Turkish government because of this new system of censoring the Internet (Arsu, 2011). The new law was criticized, alongside with previous practices over the Internet infrastructure, for a negative contrast with the democratic norms of the European Union (EU), an organization Turkey has been eager to incorporate (Kizilkaya, 2014).

Between 2013 and 2014, Turkey was in turmoil because of public protests opposed to the current government. After the police's intense reaction to tear gas, protests grew each day. With the purpose of decreasing the demonstrations, the Turkish government censored social networks sites, mainly Twitter and YouTube (Dyn, 2014d; Oi, 2014).

As mentioned before in this dissertation, during the 2013 protests, the Turkish regulator was also responsible for poisoning the DNS, concretely Google’s public address (Carstensen, 2014). Recently in 2016, the Turkish regulator, TIB, ordered ISPs to block Tor and different censorship virtual private networks (VPNs), such as VPN Master, Hotspot Shield, Psiphon, Zenmate, TunnelBear, Zero, Vypr and Express (Franceschi-Bicchierai, 2016).

3.6.7. The Russian Federation (Russia)

Russia is a federal semi-presidential republic and was considered a hybrid regime (EIU, 2011). Like the U.K and the U.S., Russia is also a permanent member of the United Nations Security Council (UN, 2014b) and its economy, the eighth largest in the world, has based on Russia's extensive mineral and energy resources, the most abundant reserves in the planet. Russia was considered a hybrid regime, but by 2017 was downgraded from hybrid to an authoritarian regime, mostly because of Vladimir Putin's decision of running (and being elected) for a third presidential term, after being also three times prime minister of Russia (EIU, 2017).

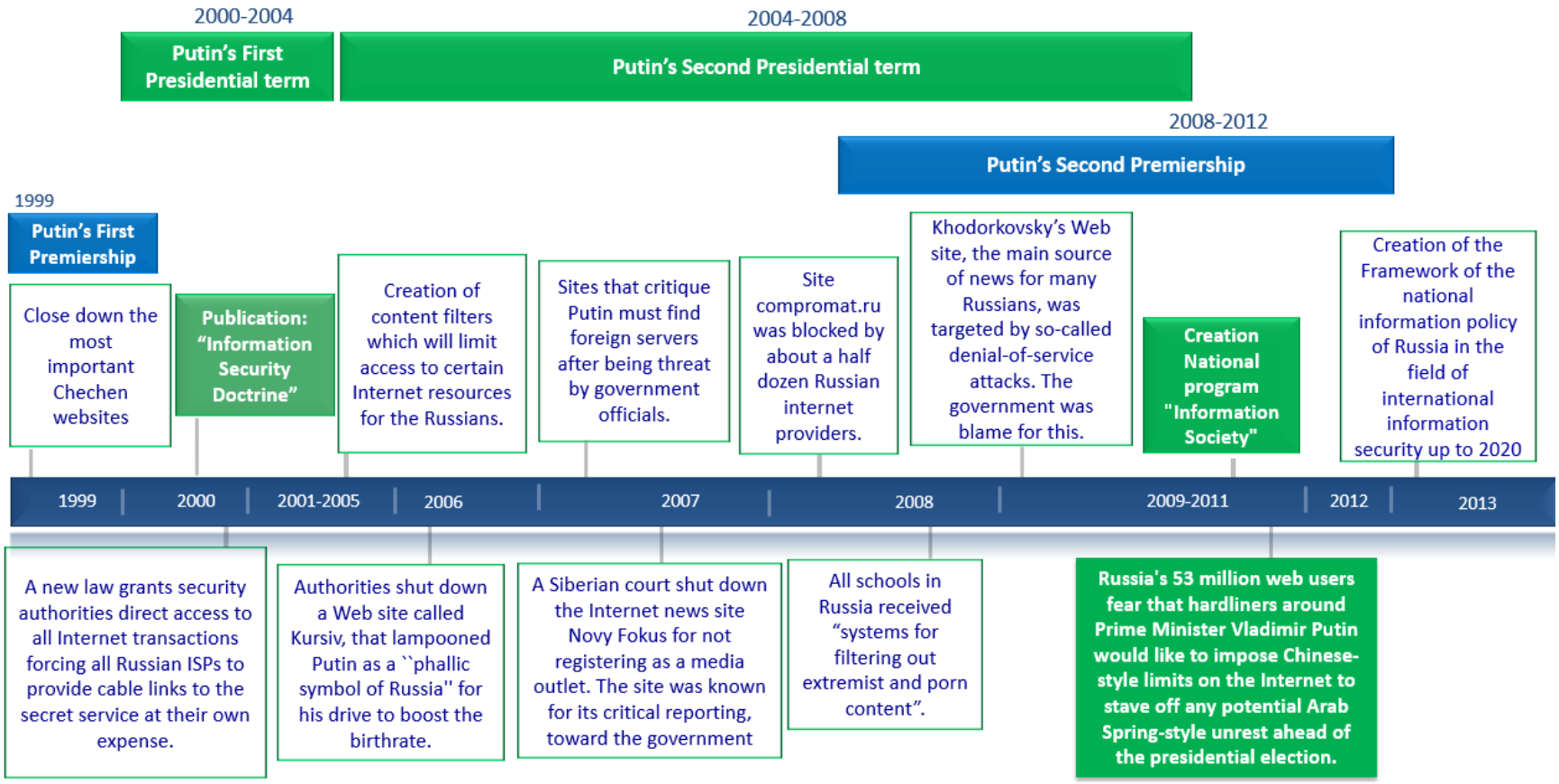
Since 2000, Vladimir Putin has remained in power either as a President or Prime Minister (Russia has both positions at the same time) and has created an oppressive policy of government control over the Internet (Morozov, 2011). Also in 2000, Putin put a law into effect that grants eight different security authorities direct access to all Internet transactions forcing all ISPs to provide information as requested (Hale, 2010).

In 2005, Russian Internet Service Providers (ISPs) were forced to provide cable links to the secret service at their own expense. Since 2006, the Russian government has implemented a robust censoring policy, and it remains today (Duffy, 2015; Morozov, 2011). Additionally, since 2012 the Russian government enacted various laws that the Moscow Times baptized the "Blitzkrieg laws" over the Internet infrastructure (Eremenko, 2014b). As part of this nationalist policy approach, the Russian Internet (российский Интернет) got its own name, RuNet (Asmolov, 2015).

At the end of 2011, Putin's second premiership also ended after he won the Presidential elections for a third administration. National protests in Russia characterized the transition between Putin's second premiership and his third presidential administration. After facing massive protests,

Putin's attitude towards the Internet shifted to gain complete control over any activity within the Internet (Please see figure 15) (Asmolov, 2015; Duffy, 2015).

Figure 15.- Russian Government Isolated Actions over the Internet Infrastructure (2000-2013)



Source: Modified from Vargas Leon, 2015

Russia has been ranked third worldwide concerning the stability of its national Internet when facing possible breaches. Only the U.K. and U.S. networks are deemed to be more reliable. RuNet has an extensive infrastructure: there are over 1,000 operators within Russian territory, with dozens of them connected to foreign networks (Kolomychenko & Kommersant, 2016).

In June 2013, after the revelation of the National Security Agency (NSA) surveillance policy[19], the Russian government called for a global protest and advocated for the creation of a U.N. body that would have regulatory control over the Internet. Mr. Ruslan Gattarov, a member of the Federal Assembly of the Russian Federation, proposed the creation of a new group to control the World Wide Web (www). Mr. Gattarov justified his request, "So that everyone, not only the U.S., has access to the master switch" (Watson, 2013, para.1). A strict interpretation of these words would suggest that the Russian legislator thought that a "real" master switch to shut down the Internet does exist.

However, this was just the beginning of a debate about the possibility of shutting down the Internet and one episode within Russian President Vladimir Putin's policy to control the Internet infrastructure. Later, between 2012 and 2014, the Russian government passed eight laws to regulate the Internet and freedom of expression in the Russian Internet. The Moscow Times baptized those laws as the Russian 'blitzkrieg'[20] laws over the Internet infrastructure because of the speed with which they were approved and the effect they had (Eremenko, 2014a).

[19]In 2013, Edward Snowden, a former National Security Agency (NSA) contractor leaked classified documents to The Guardian and the Washington Post before leaving U.S. territory for Hong Kong and then Russia. Back then, reports by The Guardian and the Washington Post reported about a program called PRISM: "collection directly from the servers" of nine U.S. Internet companies, like Microsoft (MSFT), Yahoo (YHOO), Google (GOOG), Facebook (FB), and Apple (AAPL) (Gellman, Blake, & Miller, 2013; Greenwald, MacAskill, & Poitras, 2013).

[20]Blitzkrieg or the "lightning war," is a military tactic designed to create disorganization and chaos among enemy forces by using mobile forces and locally concentrated firepower. If executed successfully, military campaigns may be shortened, which preserves human lives and limits the expenditure of artillery. During the world war II, the German forces tried out the blitzkrieg in Poland, Belgium, the Netherlands and France in between 1939 and 1940. The German commander Erwin Rommel also used the Blitzkrieg technique during the North African campaign of World War II, and it was later adopted by U.S. General George Patton for his operations in Europe (History.com, 2009).

At the beginning of 2014, the political scenario in Russia became more volatile because of the population's fear towards possible sanctions from the U.S. and the E.U. after the annexation of Crimea[21]. Despite the fact that sanctions against Russia were enacted, by September 2014 Russian officials conducted exercises to test the stability of the Internet in Russia with the purpose of making decisions that strengthen the sovereignty of the Russian segment of the global Internet (Anastasis Golitsyn, 2014a).

At the end of 2014, the Russian government started analyzing the possibility of forcing ISPs to censor content within the Internet before delivering it to Internet users. The cost of such operation was estimated in billions of U.S. dollars and is very aligned with the accusations against the Russian government of building a domestic version of the "Great Firewall of China" of web censorship (Eremenko, 2014b).

In January 2015, Vladimir Putin and members of the Russian Security Council introduced in the Russian political debate a plan that would give the Kremlin the ability to shut down RuNet from the rest of the world when Russia faces what they call a "national emergency". This reference to a national emergency includes "military actions" or "serious protest actions." In the same year, the Russian press reported that domestic ISPs blocked the traffic from various foreign sources to test how RuNet would work without them (Adam Taylor, 2016).

Russian representatives stated that the Security Council also would discuss a plan to give the Russian government control of the nation-state code top-level domains (ccTLDs), the websites ending in ".ru," ".рф," (Russian Federation in Cyrillic) and to a lesser extent ".su" (for Soviet Union) (Harding, 2014; Oleg, Kulikova, Lukatsky, Makarova, & Kolesnikov, 2017; Stone, 2014a).

[21]Vladimir Putin seized by force the Crimean Peninsula from Ukraine in early 2014. In 2016, Russia accused Ukraine of trying to stage armed incursions, but Ukraine denied it and accused Russia of massing tens of thousands of soldiers there (BBC, 2016; Treisman, 2016).

These domains currently belong to a non-governmental organization, the Coordination Centre of the National Domain, and not to the government. The Coordination Centre of the National Domain is a non-governmental organization that manages IP addresses assignments on RuNet. If Putin's intentions and the Russian Security Council are successful, the Internet shutdown policy could be a previous step to force all domains in the .ru zone to be hosted in Russia.

In the same year, 2014, Russian officials initiated the idea of creating and maintaining a "back-up-copy" of RuNet. The idea was to create a "double" (or "back-up-copy") of the Internet routing architecture, a database that would contain IP addresses, routing traffic and DNS system (Nikkarila & Ristolainen, 2017).

In June 2016, the Ministry of Communication introduced the possibility of amending the law on communication to ensure the integrity and stability of RuNet. Amendments include the need to oblige owners of all the autonomous systems that communicate traffic with foreign networks to "install technical means of control of cross-border traffic" (Kolomychenko & Kommersant, 2016). Also in 2016, Vladimir Putin's adviser German Klimenko, defended a data localization law by warning that RuNet could be disconnected from the World Wide Web (The Moscow Times, 2016).

On December 5, 2016, the Russian government call to "to deploy a national system of managing the Russian segment of the internet" (Nikkarila & Ristolainen, 2017, para.1). Moreover, Russia declared that they would develop the capabilities to disconnect RuNet from the global Internet by 2020. The task of RuNet 2020 is to stop any dependence from external networks and to secure that the Russian government gets full control over the different components of the Internet infrastructure within Russian territory. This is an act with the full purpose of achieving

what the Russians consider their digital sovereignty within the cyberspace (Nikkarila & Ristolainen, 2017).

A year later, in July 2017, Russia banned anonymous web surfing tools. The new law forbade forms of technology that provide access to prohibited websites in Russia. The ban covers services that facilitate the access to virtual private networks and proxies. ISPs are required to block sites that host these services (Deahl, 2017; Riley, 2017).

The federal website blacklist from 2012 initially only applied to sites that had content related to illegal drugs, child pornography, and suicide, but in 2017 an amendment expanded the coverage of the law to any material suspected of extremism. The change allows for broad and flexible interpretation. Therefore, the Russian government can censor any view or opinion that target its power (Deahl, 2017).

Russia has very few IXPs (29 for a vast territory) and Rostelecom, the leading long-distance-telephony-provider and close ally of the government, controls them. Previously, Russia's attempts to control the Internet were limited to securing government communications from foreign control, but in recent years that aspiration expanded to include the entire national Internet infrastructure. The Russian Security Council may try to transfer the power of the .ru and .рФ domains away from the Coordination Center of Top-Level RU Domains. The talk about shutting down the Internet is also about how to hand over control of the .ru zone from the coordination center to the government (Bodner, 2014).

For a long time, the Internet community considered that RuNet had a concentrated infrastructure, but this is not the case. Such “concentration” operates to keep the control of RuNet within Russian territory. However, RuNet also has an underlying decentralized infrastructure that

since 2013 the Russian government has tried to control through legislative and political actions (Golitsyna, Sergina, & Kozlov, 2016; The Economist, 2007).

In 2018, Klimenko claimed that the Russian government was ready to face a potential scenario where they could be disconnected from the World Wide Web (The Moscow Times, 2018).

The different statements of the Russian politicians make an echo of the words Winston Churchill had for Russia: "It is a riddle wrapped in a mystery inside an enigma; but perhaps there is a key. That key is Russian national interest." (The Churchill Society, 1939, para.1).

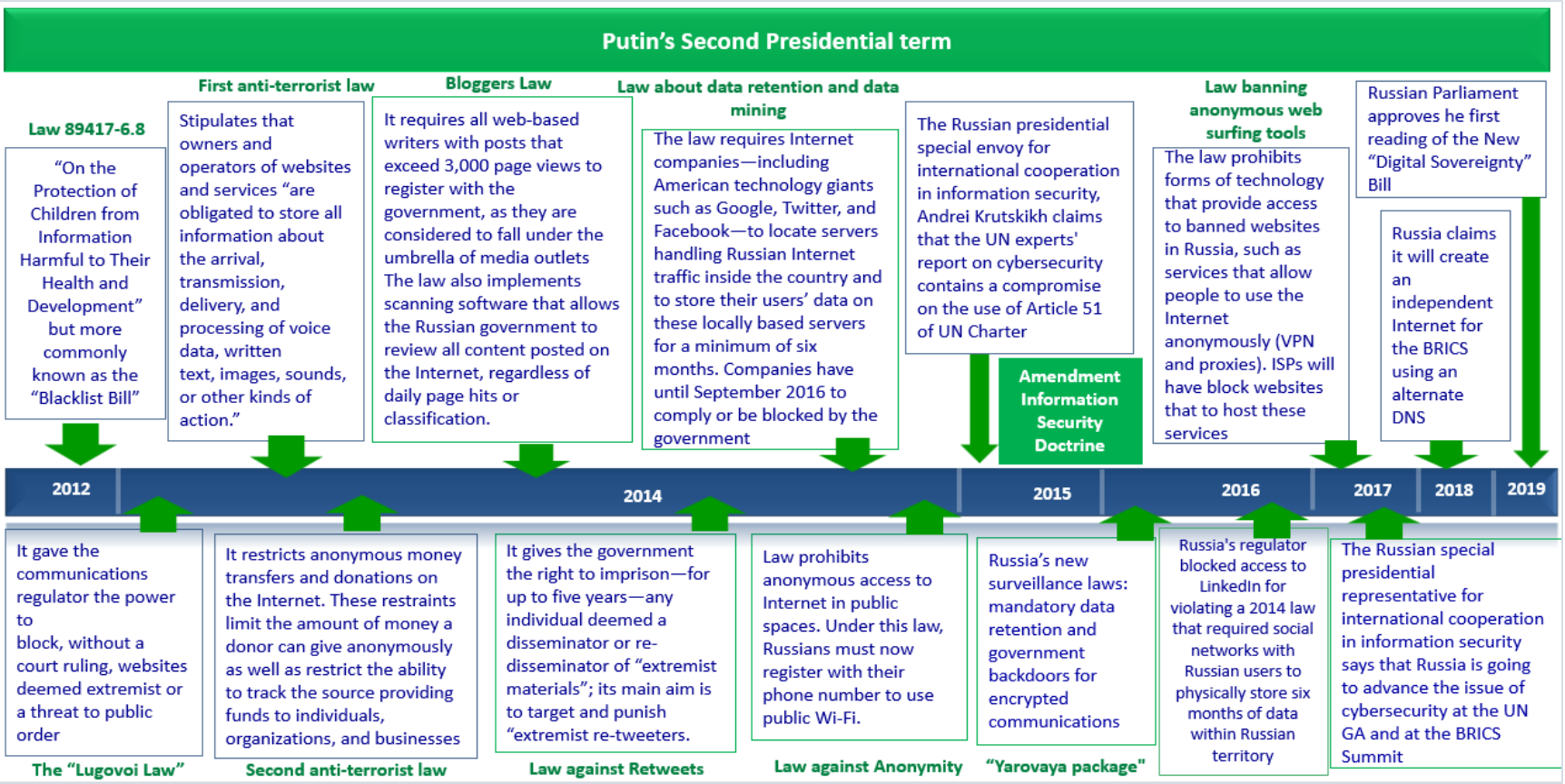
The statements of Nikiforov, Klimenko and other Russian securitizing agents indicate that Russia has at least two different approaches when considering an Internet shutdown. On one hand, there is a concern over the foreign enemy (known as the unpredictable "West") imposing its will and shutting down RuNet and on the other hand, it is the perspective of an action of the Russian government itself shutting down RuNet to protect it under circumstances of national security (Vargas-Leon, 2018) (Please see figures 17 and 18).

In the chapter 4 of this dissertation I will develop the concept of the national interest under the Russian terms and other hybrid and democratic regimes.

More recently, in February 2019, the Russian parliament passed the first reading of what has been called the "digital sovereignty bill." The purpose of this bill is to isolate RuNet from the global Internet by creating a separate internal network where both users (end-to-end) are in Russia. This would isolate RuNet from the global Internet, a condition that (in the Russian mindset) would protect the traffic and would make it less vulnerable to interception. This condition also would provide a degree of resilience against cyberattacks from a foreign power. To achieve this condition as an independent network, RuNet would require its own DNS. and cross border mobile and

satellite connections to ensure that the integrity of the network was maintained. By closing international connections, traffic from abroad must be monitored and filtered (Venables, 2019).

Figure 16.-Russian 'Blitzkrieg' Laws and Actions Over the Internet Infrastructure (2012-2019)

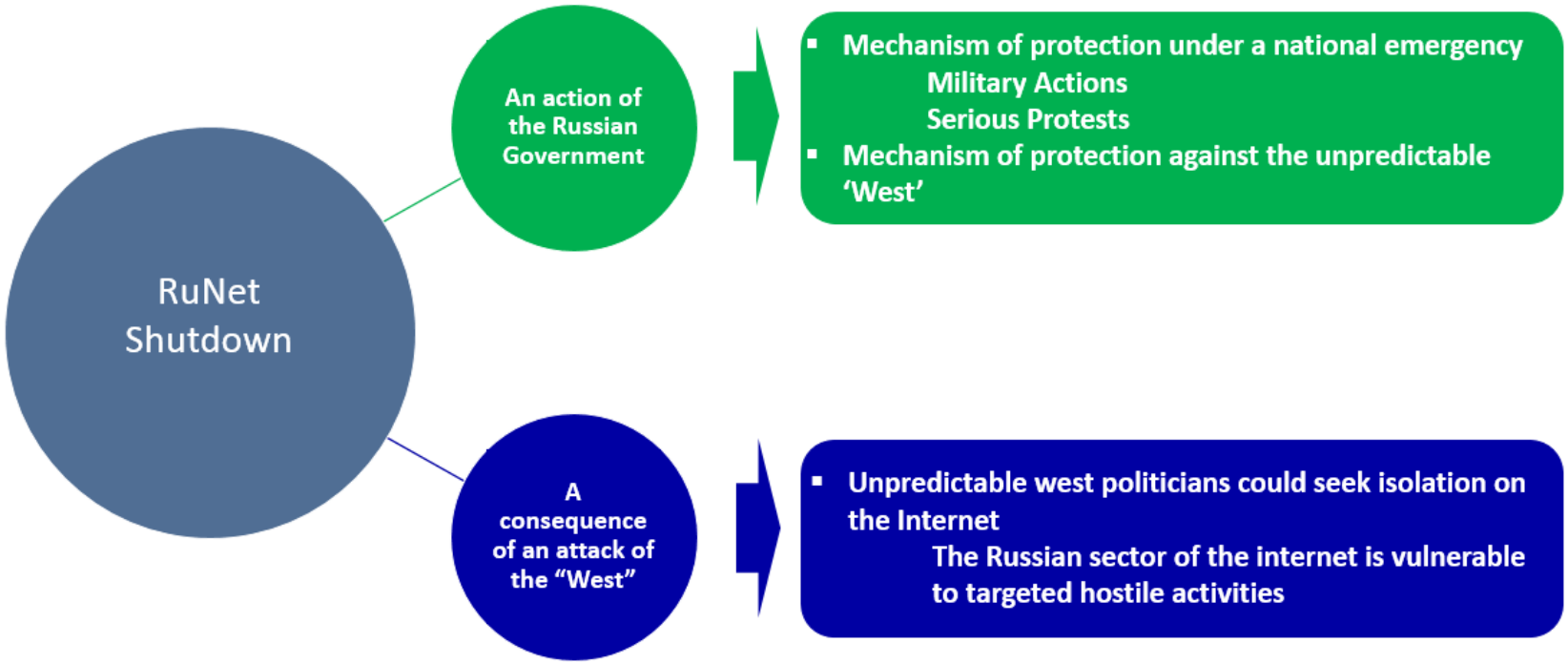


Source: Updated from Vargas Leon, 2015

Figure 17.- Russia Internet Shutdown Bill and Further Actions (2013-2018)

Source: Updated from Vargas Leon, 2015

Figure 18.- Russia Perception over the Shutdown of the Russian Internet (RuNet)



3.6.1. República Federativa Do Brasil (Brazil)

Brazil is a republic with a federal presidential constitutional system and is the largest economy in the South American hemisphere and the world's seventh largest one. Brazil also has one of the world's fastest growing major economies, and its economic reforms gave to that nation-state international recognition and influence (IMF, 2014).

Despite its economic progress, the EIU classifies Brazil as a young democracy because of its low levels of political participation and government actions over the freedom of speech on the Internet as I will describe in the following paragraphs (EIU, 2011, 2017). In August 2016, the Brazilian Congress impeached the president Dilma Rousseff, of the left-wing "Partido dos Trabalhadores" (The "Workers' party") for allegations of corruption and contravening budget rules (this case is known as the Petrobras corruption investigation). This party held power since 2003, and Dilma Rousseff was replaced by Michel Temer, who may not see out his term of office until end-2018 because he has also been indicted for cases of corruption (EIU, 2016).

From a technical point of view, since 2004 Brazil has taken significant steps to create a national system of "Pontos de Troca de Tráfego" – PTTs (in English: Traffic Exchange Points), which is a network of Internet exchange points located in every major metropolitan area. These IXPs make easier and less expensive for Brazilian companies and Internet users to connect to the Internet. They use the BGP routing system to allow multiple services from different ISPs, and in that way, they reduce their dependence on a single ISP (Cowie, 2015; Dyn, 2014a).

Despite the technical progress creating a robust Internet network, in legal terms, the situation is very controversial. Between 2006 and 2007, a court ordered to the most prominent Brazilian ISPs to block specific sites, and later in 2007, YouTube IP addresses were blocked on its backbone due to a court decision. Additionally, in December 2007, a court forced a journalist

to withdraw content from an Internet site that implicated a state representative (OpenNet, 2013). Between 2008 and 2013, multiple court orders affected the Internet, by blocking sites with apparently defamatory and homophobic content. In the last case, the government also demanded that hosting services divulge the identities of users who post offensive material. Within the same period, Google was required to take down Orkut communities (the most popular social network in Brazil at the time) that could be considered offensive to an evangelical minister (OpenNet, 2013). Similar practices have continued until 2018.

In 2013, after the Snowden revelations, Brazil emerged as an enemy of international surveillance practices and called for an international conference, known as NetMundial. In that conference, the Brazilian government invited to create a global Internet governance regime where developing nation-states should be represented (Barbara, 2013; Keating, 2013a). Additionally, the Brazilian Congress enacted what is known as the Brazilian Internet bill of rights, the "Marco Civil" legislation. Marco Civil includes two fundamental principles, such as the privacy online and the network neutrality, which forbids the discrimination of the Internet packets (Moncau & Mizukami, 2014; Peralta, 2014).

After the Snowden revelations, Brazil also became a champion of the "cyber-nationalism," advocating for the protection of their citizens' data by keeping it stored in servers within Brazilian territory. At some point, there were calls to create a separate Internet from the one created by the U.S. (Keating, 2013a, 2013b). Between 2015 and 2016, the online censoring policy in Brazil increased, by blocking WhatsApp, Facebook, Twitter and YouTube multiple times, and many of them with the assent of the Court system (Olukotun & Pallero, 2016; Pallero & Olukotun, 2015). The main excuse for censoring the Internet content in Brazil has been the fight against cybercrime

(ITS Rio, 2016). Since 2016, after President Dilma Rousseff was indicted, online censoring in Brazil increased (Pallero, 2016).

On August 8, 2017, the new Brazilian administration (the Temer administration), published a public consultation in the Official Brazilian Gazette "Diário Oficial da União" - D.O.U. (Federal Official Gazette of Brazil - F.O.B.). The public consultation aimed at changes in the composition, election process and powers of the Internet Steering Committee (CGI.br) (Direitos Na Rede, 2017). CGI.br is a managing committee, an organization, composed of representatives of the government, the private sector, civil society, and technical and academic members. CGI.br was created to establish standards and procedures for the use and development of the Internet in Brazil and is also responsible for defining the guidelines for all issues related to the Internet regulation (CGI.br, n.d.).

CGI.br also serves as a technical resource to legislators and the executive branch, especially on issues related to network neutrality, data protection, universal access, and privacy online. Because of these compelling attributions, CGI.br is considered a threat to some government officials who would prefer less scrutiny over Internet policies (Direitos Na Rede, 2017; Segal, 2017). The public consultation has been criticized because the government unilaterally attempts to change the composition of CGI.br, without any dialogue with the other members of the Internet ecosystem represented in CGI.br (Segal, 2017).

At this point, it is important to note that despite so many censorship episodes and attempts of control over the Internet infrastructure, Brazil never considered or mentioned the possibility of shutting down the Internet. On the contrary, when the Brazilian government discussed this issue was to deny any possibility of shutting down the Internet categorically. The discussion occurred previously to the world soccer cup and the Olympic games to be held in Rio and other cities of Brazil in 2014 and 2016 respectively. The Brazilian government denied any possibility of shutting

down the Internet, and they were also preparing to prevent any chance of an Internet shutdown provoked by a third party (Carpes, 2012; CEPROMAT, 2014).

3.6.2. Estados Unidos Mexicanos (México)

Mexico is a federal republic in North America and is the fifth largest nation-state in the Americas. Mexico's economy is firmly connected to the North American Free Trade Agreement (NAFTA) (The Catalist, 2010). In 2000, after 71 years, the PRI (Partido Revolucionario Institucional - Institutional Revolutionary Party) lost a presidential election to Vicente Fox of the opposition. In the 2006 presidential election, Felipe Calderón from the "Partido de Acción Nacional" (PAN) (National Action Party) was declared the winner, with a very narrow margin over the leftist candidate Andrés Manuel López Obrador. In 2012, the PRI came back to power with the candidate Enrique Peña Nieto (today's President in 2017) (Miroff & Booth, 2012). Initially, President Peña Nieto introduced himself as an active President fighting against the drug dealing in Mexico. However, after multiple scandals of corruption and human rights violations, his administration has been questioned and criticized by international organizations and the international community (Ackerman, 2016; Miroff & Booth, 2012).

Mexican policy over the Internet infrastructure has been driven by stand war against drug traffic because the cartels use the Internet and social networks to distribute the illegal narcotics actively (El Comercio, 2016; OpenNet, 2013). Additionally Mexico also has to fight against cybercrime and child pornography on a large scale (Comision de Atencion a Grupos Vulnerables, 2014). In 2013, the Mexican government announced that the Peña Nieto administration would

create an intelligence strategy to identify information available on the Internet that could be helpful to track criminals. Representatives of the government stated that:

> "Esta información que se genera en la actividad cibernética (…) tiene que sistematizarse, tiene que aprovecharse y tiene que utilizarse para poder combatir a los delincuentes" (Montalvo, 2013, para.4)
>
> *Translation:*
> The information that is generated within the cybernetic activity (...) has to be systematized, has to be exploited and has to be used to be able to fight criminals."

In March 2014, the Mexican Executive branch prepared an amendment to the Federal Telecommunications Law. The Executive proposed a new chapter called "Collaboration with the Justice System". According to the proposal, the telecom providers would be forced to provide the geo-localization in real time of any device requested by the authorities and those authorities were entitled to interfere with private communications (Garcia Martinez, 2014). Interception of private communications for reasons of national security and justice is allowed if there is a previous warrant for that purpose. However, when is about geo-localization, a warrant won't be required if the crime under investigation is related to crimes against health, kidnapping, extortion or the life of the victim is threaten (Ángeles, 2013).

According to this proposal, telecom providers should keep a record of the interventions of the communications and should keep the name of the user, domicile, type of connection, date, hour and place of geo-localization. If authorities request, the telecom providers must suspend the service of the mobile devices, block, inhibit or annul the telecommunication temporarily in events and critic events when the national security is involved. This draft was the text of the article 196 of the project, which was supposed to be amended according to the article 5 of the Mexican national security law, which establishes that telecom providers are required to provide any information related to any device to the authorities. In the specific case of the Internet, telecom providers were

supposed to prevent the expansion of non-requested massive electronic communications or "malicious traffic". The context for this amendment, just like the justification, was the fight against three major crimes: cyber-crime, human trafficking and drug dealing, mainly the last one. Facing strong opposition from the civil society and the private sector, the amendment did not pass (Garcia Martinez, 2014; Ramos, 2014).

Despite this strong surveillance policy of the Mexican government, it is also important to note that the article 6 of the Mexican Constitution grants to the Internet the condition of human right.

> "Constitución de los Estados Unidos Mexicanos de 1917 y Modificaciones Constitucionales del 2013"
>
> "Título Primero Capítulo I De los Derechos Humanos y sus Garantías"
>
> "Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado. Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión. El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios"
>
> "…"

Translation:

> Constitution of the United States of Mexico from 1917 and Amendments from 2013
>
> First Title.- Chapter I About Human Rights and their Guarantees
>
> Article 6.- …
>
> The manifestation of ideas will not be subject to any judicial or administrative proceeding, but if attacks morals, private life or the rights of third parties cause crime or disrupts public order; the power of reply shall be exercised in the terms established by law. The State shall guarantee the right to information. Everyone has the right to free access to plural and timely information, as well as to seek, receive and impart knowledge and ideas of all kinds by any means of expression. The State shall guarantee the right of access to information and communication technologies, as well as

> to the broadcasting and telecommunications services, including the broadband and internet. For these purposes, the State shall establish conditions of effective competition in the provision of such services
> …

This constitutional amendment became effective in 2013 (Becerra, 2008). Regarding this constitutional protection, which has no limit or exception, an action to shut down the Internet in Mexican territory or law that allows it, would be both unconstitutional.

4. Analysis and Findings

The next chapters present the results of the study conducted for this dissertation, which aimed to answer RQ1, RQ2, and RQ3. The first section includes the global scope of the Internet shutdowns, what governments executed an Internet shutdown and the ones that considered doing it. The second section comprises the rhetoric of governments that shut down or considered shutting down the Internet, the justifications they provide to apply this extreme form of government control. To analyze these justifications, I use as a theoretical framework the Copenhagen securitization theory. The last part includes a description of the political, legal and technical factors that enable a government to shut down the Internet or to consider doing it.

4.1. Answer RQ1: What is the Global Scope of the Internet Shutdown Phenomena?

The first research question of this dissertation addresses the global scope of Internet shutdowns. I present my results in the graphics below (figures 19 and 20). The first graphic was from 2014 when this project was at an early stage, and the second is from March 2018.

4.1.1. Internet Shutdown Cases

Considering the previous analysis, I will report the global scope of the Internet shut down in the next figures. Results are classified into two groups:

1. Cases when an Internet shut down occurred, and if the shutdown was national or concentrated in a specific city. On this matter, colors differentiate the type of regime and if the shutdown covers a town or the entire territory of a nation-state. I report these cases in the upper part of the slide.
2. Cases where there were considerations about an Internet shut down. In this case, colors differentiate between the type of regime and the government discourse related to the Internet shutdown. I report these cases in the lower part of the slide.
3. Special situations to mention include the following ones: when there was an Internet shut down, and there were government claims of an accident and when there was an Internet shut down, and the local government claims that it was the result of an attack of cyber warfare or if an alleged case of cutting a fiber cable existed.

Figure 19,- Global Scope: Internet Shut Down Cases, 2005-2012

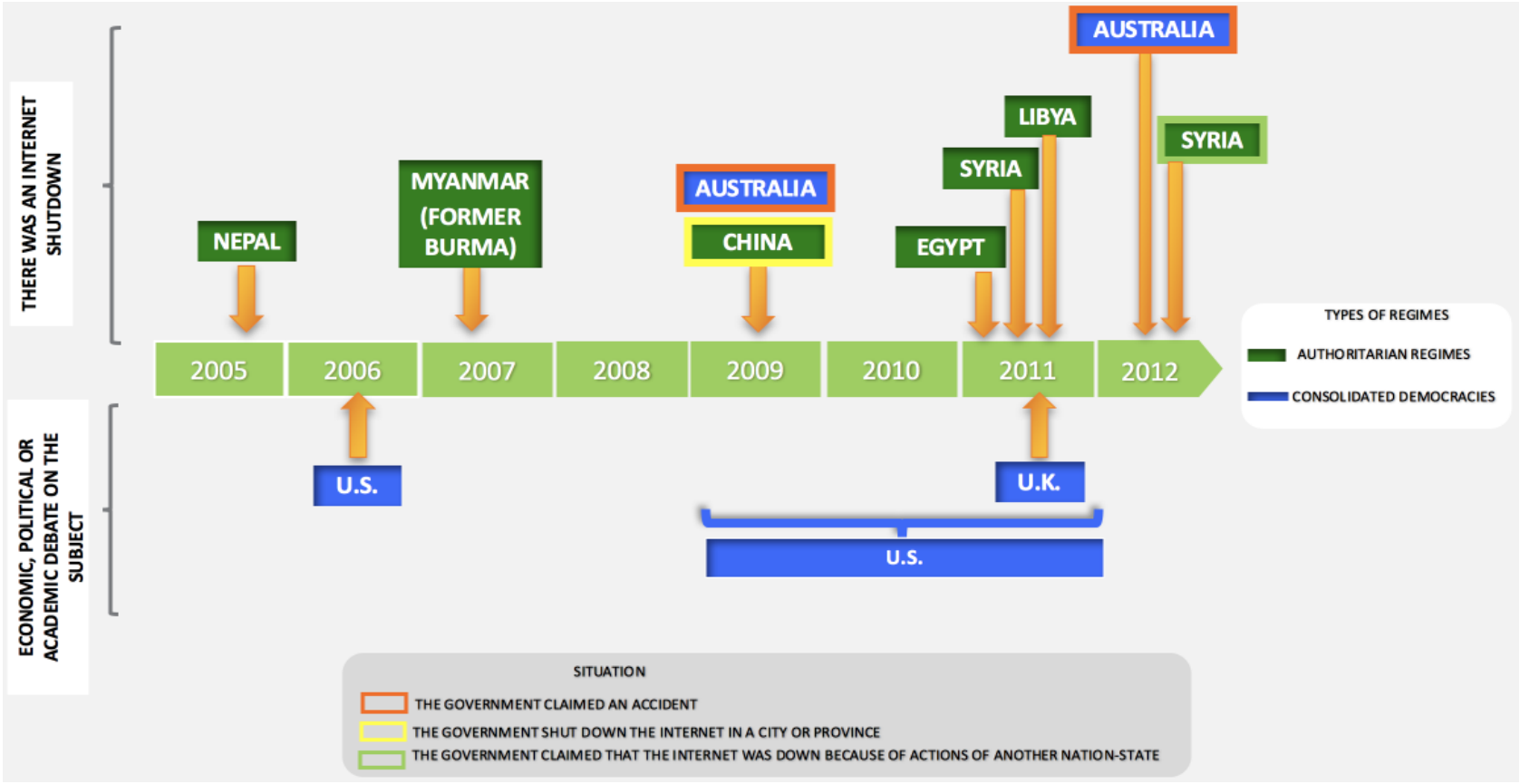
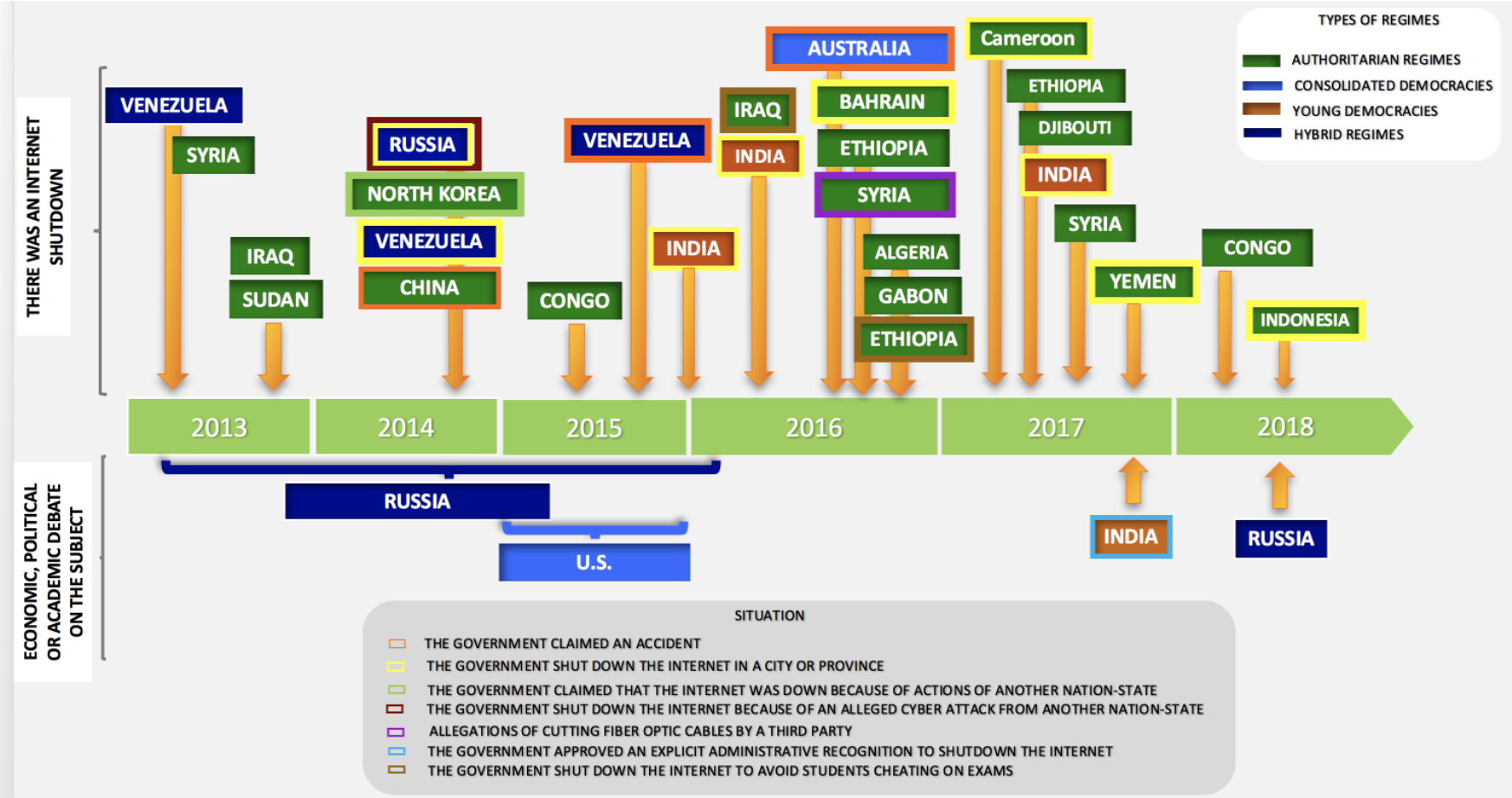


Figure 20.- Global Scope: Internet Shut Down Cases, 2013-March 2018



As the previous graphics portraits, according to this dissertation, the global scope of the Internet shut down is as it follows:

1. Approximately 18 authoritarian regimes were involved in an Internet shutdown. Some of these regimes were engaged in more than one episode to shut down the Internet: Nepal, Myanmar (former Burma), China, Libya, Egypt, Syria, Iraq, Sudan, North Korea, Congo, Bahrain, Ethiopia, Algeria, Gabon, Cameroon, Djibouti, Yemen and Indonesia.
2. One consolidated democracy and one young democracy, Australia, and India were involved in an Internet shut down on more than one occasion. Australia always claimed an accident
3. One hybrid regime, Venezuela, was involved in an Internet shut down on at least three events
4. Three consolidated democracies, Australia, U.S. and U.K., were engaged in political, legal or academic debate to provide power to their government authorities to shut down the Internet
5. One hybrid regime, Russia, was involved in a legal and political debate to give power to their government authorities to shut down the Internet
6. One hybrid regime, Russia, shut down the Internet in one of its cities (Crimea after the annexation) alleging a cyberattack from Ukraine
7. Two dictatorial regimes, Syria and North Korea, claimed their Internet was shut down by another nation-state
8. One young democracy, India, created administrative rules that allow the government to shut down the Internet

4.2. Answer RQ2: What Justifications Do Democratic and Hybrid Regimes Use to Shut Down or to Consider Shutting Down the Internet?

To answer RQ2, this dissertation understands as "justifications" the arguments to endorse a particular proposal, law, policy or regulation (Vallier & D'Agostino, 2013). To identify those arguments this dissertation conducted a rhetorical analysis of the securitizing speeches of those who are known as securitizing agents, regarding the Copenhagen securitization theory. These speeches are related to an Internet shutdown as an extreme measure to protect the national interest. As mentioned before, in this context, this dissertation understands as speech a set of expressions, written or spoken, that comment about one or more government actions, that is both intended and received as a contribution to public deliberation (Niedrich, 2011).

The securitization theory describes speech in the following terms: by referring to the urgency of action posed by an existential threat, a securitizing actor can transform (through speech) an issue into one of security and can attempt to make anything a referent object. A referent object is that thing that must be protected to preserve the national security and therefore, the survival of the nation-state (Buzan, 1998).

For this dissertation the extraordinary measure is the act of shutting down the Internet. The audience, securitizing actor and referent object vary according to the specific case under analysis. The next paragraphs will identify these three elements of the theory in the selected case studies and will answer RQ2.

4.2.1. Securitizing Actors and Speech

A securitizing actor is one who "securitizes" something, by declaring it a "referent object". As explained in the first chapter of this dissertation, a securitizing actor is either a person or group who performs the security speech-act. However, this speech-act only can be performed by an actor in an authoritative position, a person or group of people who: a) have both, authority and legitimacy to be heard and believe for the targeted audience, and b) have the capacity to adopt measures to deal with the "security problem". The existence of these conditions limits potential candidates for securitizing actors to governments, leading politicians and maybe scientific experts or technocrats. (Buzan, 1998; Rothe, 2015).

As I established while collecting data, when is about Internet shutdowns, securitization agents belong to different government sectors: a) leaders of the executive branch, the President or Prime Minister. Claims also correspond to heads of national security agencies and ministers, b) members from the legislative branch, congress members and, c) civil servants. Statements, either written or spoken, refer to the need of having a policy like an Internet shut down and reasons to act accordingly. In terms of national security, their role is to establish a concept of what the national interest is because the protection of the national interest is necessary to guarantee the survival and functionality of the nation-state. In terms of the theory, the national interest is called "referent object," the thing or things that, according the security agents, must be protected to guarantee the national security of a nation-state.

Audiences vary depending on the nation-state and whether it is a hybrid or democratic regime. The securitizing agent must convince a specific audience that they are the "agents of change," because without them, without their participation, is not possible to protect the national interest.

The extraordinary measure, in this case, is the act of considering or shutting down the Internet because there is no any other thing that can be done to protect the national interest.

To provide an example of the application of this theory, I will refer to the work of Myriam Dunn Cavelty (2008), about the securitization of the cyberspace by the U.S. government. Dunn Cavelty explains how cyber threats moved very quickly into the U.S. political agenda. Cyberthreats are defined as "a rather vague notion signifying the malicious use of information and communication technology (ICT) either as a target or as a tool by a wide range of malevolent actors" (Dunn Cavelty, 2008, p.1).

The use of cyberthreats constitutes part of the speech-act while policy entrepreneurs and professionals of security turned into securitizing agents because they can create or frame the discourse. The reason for the speech-act is straightforward: cyber threats are a new threat to national security and the foundations of developed societies. The referent object (or national interest), according to Dunn, is formed by governments and private systems as cyber threats attack directly to them and those systems are part of the functionality of a nation-state. Government top decision-makers build the audience, as they are the ones who created this securitization policy over the cyberspace. The extraordinary measure (a failed one according to Dunn) is the securitization of the cyberspace and the use of any possible action to fight a cyberattack (Dunn Cavelty, 2008).

4.3.2 Analysis and Selection of Cases for Rhetorical Analysis

RQ1 provided this research with a global scope of the Internet shut down phenomena. Cases under analysis to answer RQ2 are the ones that shut down the Internet or considered doing so because they are the ones where their government representatives discussed the subject. In the

group of the democratic regimes are the U.S., U.K., and Australia. In the group of the hybrids are Russia and Venezuela.

The selection criteria previously explained to include and exclude sources identified around 3,000 documents for the entire analysis. The materials corresponding to Australia, U.K., U.S., Russia, and Venezuela make around 2,019 (these are the nation-states that shut down or considered shut down the Internet). I analyzed those documents using the software ATLAS.ti. For this purpose, I created five projects within the software, one per nation-state.

Categories for analysis belong to the rhetorical analysis: 1) rhetor, 2) purpose, 3) audience, 4) evidence and 5) strategies (Campbell, 2009). The identification of these categories allowed us to establish the elements of the securitization theory: purpose (I start by the point that a securitizing actor must convince an audience that shutting down the Internet is necessary to preserve the national interest), audience, why this extraordinary measure (shutting down the Internet) is essential and the elements to support such claim (See below, table 03). I will explain the evidence and strategies as elements of the speech.

Table 03.- Elements of the Securitization Theory and its Correlated Elements in the Rhetorical Speech Analysis

Units of Discourse Securitization Theory Copenhagen School		Categories of Analysis Rhetorical Speech	
Securitizing Agent		**Rhetor**	
Speech Act	Grammar of Security (protection of the Referent Object) Threat Subject Extraordinary Measure	Rhetorical Speech	Purpose Evidence Strategy
Audience		Audience:	Agents of Change Created Audience

After I identified each one of the categories of the rhetorical analysis, I added them to a specific group, whether they belonged to hybrid or democratic regimes. By including these categories into groups, it is possible to identify the elements of the security discourse that belong to each type of political regime.

At this point, it is important to remember that, as mentioned before, this dissertation relies upon security speeches available on the Internet. Because of this characteristic, I triangulated the data. This process was necessary to increase the credibility of the research results (Yin, 2009). The process to select the sources was explained in detail when presenting the exclusion and inclusion criteria.

4.3.3. Securitizing Actors and Speech

The next paragraphs will describe the results of the analysis using ATLAS.ti. I will present the findings of this project in the following chapters according to the type of regime (consolidated democracy or hybrid) and the elements of the theory: securitizing actor, the audience they intend to address and aspects of the securitizing speech (I will include evidence if any, and strategy will here).

4.3.3.1.Audience

According to the terms of the securitization theory, the audience is formed by people or organizations that have to be convinced by a securitizing agent that an extraordinary measure is

required to protect the national interest (the "referent object" in terms of the theory) (Buzan, 1998). The identity of the audience depends on the context of the securitization process and its capacity to legitimize the actions proposed by the securitizing actor. The role of the audience is central because securitizing actors and audiences are in constant interaction and because audiences actively engage and have a role in the securitization process. Audience members actively participate in the construction of the discourse interacting with the securitizing agent. While the actions and influence of audiences vary across cases, audiences have, at least, the potential to exert influence over securitization processes and the policies selected to address potential threats (Côté, 2016).

As mentioned before, initially the securitization theory defines the audience as those who have to be convinced of the securitizing move to be successful (Waever, 2003). The audience also can be defined as the individual(s) or group(s) that has the capacity to "authorize the view of the issue presented by the securitizing actor and legitimize the treatment of the issue through security practice" (Côté, 2016, p.548). However, audiences not always legitimize or agree with the security speech. Audiences either: 1. Challenge the securitizing actor's presentation of what should be a national security issue; this forces the securitizing actor to create or modify a security narrative, or 2. They provide moral support to the securitizing move (Côté, 2016; Vuori, 2008).

In any case, audience(s) are essential because of their capacity or ability to provide what the securitizing actor needs to accomplish or reformulate the securitization process (Vuori, 2008). Following the terms of the securitization theory, the rhetoric classifies the audience in two types: 1. Agents of Change and 2. Targeted Audience. The individuals of the first group, the agents of change, are the ones that can do what securitizing agents want. They are the ones who have the power to act, whether it is political, economic, or social. The second group, the individuals of the

targeted audience, are very likely to be responsive and may or may not share some basic assumptions with the securitizing agent to buy the securitizing speech (Campbell, 2009; Côté, 2016; Vuori, 2008).

The analysis of this research under the terms of the securitization theory starts considering the Internet shutdowns as an extraordinary measure, the action to be executed to protect the national interest. Moreover, as it will be explained in the next paragraphs, for the cases under study, the audience is always the private sector, but precisely who in the private sector is an actor, will change depending on the type of context and regime. In the next paragraphs I will analyze both cases, well-consolidated democracies and hybrid regimes.

4.3.3.1.1. Consolidated Democracies

Part of the academic sector has established that consolidated democracies became increasingly worried about the protection of the critical infrastructure since the September 11, 2001 attacks in the U.S. The critical infrastructure is basic to preserve the integrity, functionality and survival of a nation-state. It is also the case that in consolidated democracies, the private sector is the one that owns and handles the critical infrastructure. Therefore, the private sector is a constant actor within national security policies of democratic regimes (Eckert, 2005; Giacomello, 2005, 2016; Radvanovsk y & McDougall, 2009).

As I will explain in the next paragraphs, the private sector is also the audience to convince when a national security emergency is in place and shutting down the Internet becomes an option. It is important to point out the private sector this dissertation considers as the audience, in terms of the Copenhagen securitization theory, is the private sector that owns and handles the critical

infrastructure, so vital for the stability of the nation-states during the 21st century. I will develop this conclusion in the next paragraphs. I will explain now each case separately.

Back in 2011, during the Arab Spring, the former Australian Minister for Broadband, Communications and the Digital Economy, Stephen M. Conroy, denied any government attempt to shut down the Internet in Australia:

> "Australia's a vibrant democracy, where the government doesn't control the internet ...I don't think we have any of these powers — that we could pass a law to make ISP services turn off when we want them to? I don't think we have that power now, and I don't think anyone's seeking it." (LeMay, 2011, para.6)

Mr. Conroy pointed out to the ISPs as the ones in control to accomplish an Internet shutdown. On this matter, it is important to clarify that, generally, consolidated democracies have massive communication networks, nevertheless when is about ISPs, the situation has a clear distinction: the U.K. has around 3,000 ISPs and the U.S. has between 3,500-4,000 ISPs. However, in both cases, four big corporations have the power to control around 70% of the Internet users. In Australia, the former-government-owned Telstra handles around 90% of the Internet subscribers and 44 additional ISPs, that cover 10% of the remaining subscribers, depend on Telstra's proper functionality (Hernandez, 2014; Ryter, 2009). In all democracies, most of the Internet service is concentrated in one or few ISPs.

In this scenario, and despite Mr. Conroy's words rejecting an Internet shutdown, since 2011, Telstra has reported at least three Internet shutdowns. In all those three instances Telstra claimed an accident, a human error, or denied knowing what produced the Internet shut down. Since Telstra handles around the 90% of the Internet subscribers in Australia, almost all Internet users in that nation-state were affected (Kidman & Allen, 2012; LeMay, 2011):

Author: Big Pond, a division of the telecommunications company Telstra (Australia) (2011)	“We are currently having problems with the BigPond Self Care Portal. This is affecting customers nationally. Customers may be unable to login and manage their accounts. Technicians are treating this issue as a priority and are working on the problem” (Didymus, 2011)
Author: Telstra representative (Australia) (2012)	"At this stage, we understand [Dodo] began to present an excessive number of IP routes, and the configuration of Telstra's core network (Telstra Internet Direct) allowed this to overload the Telstra network," (J. Taylor, para.5, 2012) "Service was restored by removing the impact of excessive routes" (J. Taylor, para.5, 2012)
Author: Telstra representative (Australia) (2016)	“We are aware of an issue impacting some business and enterprise customers in Victoria,” “We are investigating the cause and working to restore services as soon as possible” (Frankland, 2016)
Author: Telstra Chief operations officer Kate McKenzie (Australia) 2016	“the failure was an embarrassing human error after a node, which manages network traffic, malfunctioned on Tuesday morning” (Hunt, 2016)
Author: Telstra representative (Australia) (2016)	“A lot more than that were worked on this morning ... which is human error” (Hunt, 2016)

Because of the large volume of Internet subscribers that Telstra handles, other ISPs also become inoperable when Telstra is down and the international traffic also gets compromised (Lohman, 2011).

Up to this point, Internet shutdowns in Australia seem to be the outcome of an accident, or at least, that is what the justifications indicate. However, private companies and civil society organizations have questioned all episodes of Internet shutdowns in Australia not only for its frequency but also because these technical failures were never clearly explained (Chester, 2016; Frankland, 2016; Kidman & Allen, 2012; Koerber, 2016; Stiles, 2016).

Additionally, when the Internet shutdowns occurred in Australia, members of the private sector questioned the functionality of Telstra and remembered the opinions about the Internet regulation that Mr. Cameron pronounced in 2010:

Author: Former Minister for Broadband, Communications and the Digital Economy Stephen M. Conroy (Australia) (2010)	[The Internet] "It's a communications system. It's not magic. I know there are people who like to give it magical properties, net utopians think that it should be completely unregulated," "This government and many other governments around the world don't accept that argument." (LeMay, 2010a, para.3)

Although Mr. Conroy opposed to any international regulation of the Internet, he never objected a robust national regime where the government, the sovereign one, has strong policies over the Internet infrastructure, which includes the ISPs and every single operator involved in the Australian Internet infrastructure (LeMay, 2012).

When denying any possibility of shutting down the Internet, Mr. Conroy referred only to the Internet service providers (ISPs) as main actors who could not be constrained or ordered by the government to exercise that extreme policy. However, at the same time, he also claimed that the Internet couldn't be de-regulated. Following this line of discourse, since early 2010 until 2016, Conroy tried to implement censoring policies within Australian territory, and he declared his distrust publicly to the ISPs that run the Australian Internet (LeMay, 2010a, 2010b).

In 2015, following the Chinese attacks into Bureau of Meteorology's systems[22], the Australian government claimed that hacking costs $1 billion annually to the national economy.

[22] Back in 2015, the Australian Bureau of Meteorology (BOM) claimed, after a report by the ABC about a large breach, that its systems were fully operational. ABC claimed that the source of attack was China, but the Australian government didn't comment on the subject (Duckett, 2015).

Also in 2015, the Australian government prepared a draft of legislation requiring to ISPs to increase network protection and to increase oversight to government agencies to intervene for national security (Duckett, 2015; Reichert, 2015).

In April of 2017, the government released a $230 million domestic cybersecurity strategy that involved collaboration between public and private sectors. However, the private sector in this strategy includes the owners of the Australian critical infrastructure (Yoo, 2017). Dan Tehan, the minister of defense personnel at the time and, also responsible for assisting the prime minister in cybersecurity issues launched the first joint cybersecurity centre. Mr. Tehan reinforced the importance of the private sector, the owner of the critical infrastructure:

> "Securing Australia's cyberspace is not something the Commonwealth can do alone. This collaborative approach will provide up-to-date information about the nature of cyber threats, help partners better understand cyber risks, and allow them to collaborate on shared challenges," (Yoo, 2017, para.5)

As I mentioned before, audiences are essential for the securitizing agent because they provide what the securitizing actor needs to accomplish the securitization process (Vuori, 2008). From the words of Mr. Conroy, the control of ISPs is vital because they can grant access to the Australian critical infrastructure through the Internet. Although the ultimate purpose of the Australian government is not shutting down the Internet, but to protect the critical infrastructure of that nation-state, shutting down the Internet may be one of the means to do it.

According to the government's view, ISPs became instrumental for the final purpose. The government needs them to accomplish an Internet shutdown as they are key for the population connectivity (at least in Australia where Telstra controls most of the Internet market). However, although the ISPs are instrumental in achieving an Internet shutdown, they are not the audience. The audience in this case is the private sector, the owners of the critical infrastructure and the

Internet infrastructure. They are the agents of change (in terms of the securitization theory) not only because they are instrumental achieving an Internet shutdown, but also because the threats over the critical infrastructure are the drivers of the Australian national security policy. In that case, their situation and allegations are important components of the securitizing speech.

On the other hand, the U.K. and the U.S. have similarities in one point: both regimes, at some end, explicitly agreed that shutting down the Internet was acceptable. The purpose of such extreme policy is the protection of the critical infrastructure (see quotations below). As mentioned during the description of the case studies for this project, the U.S. Senate considered three bills when it was about an Internet shutdown: S.773, S.3480, and S.413. The White House also had its proposal on the subject. The next paragraphs will analyze the arguments of the sponsors of these bills and the White House representatives.

The sponsors of the referred documents stressed the fact that protecting the critical infrastructure only can be achieved with close collaboration with the private sector because the private sector owns and handles most of the critical infrastructure within U.S. territory. Without the private sector shutting down the Internet cannot even be considered in a land with a massive Internet infrastructure like in the U.S.

The first bill, S.773, was sponsored by Senator Rockefeller[23] and was introduced in the Commerce, Science and Transportation Committee of the U.S. Senate in 2009. S.773 was the most controversial bill because it explicitly provided powers to the president to order the shutting down

[23] Cosponsors of the bill include: (Civic Impulse, 2017)
Nelson, Bill [D-FL] (joined Apr 1, 2009)
Snowe, Olympia [R-ME] (joined Apr 1, 2009)
Bayh, Evan [D-IN] (joined Apr 2, 2009)
Mikulski, Barbara [D-MD] (joined Apr 22, 2010)

of the Internet[24]. Because of the extreme opposition from the private sector and the civil society, sponsors of the bill removed that provision from the original draft.

Senator Rockefeller explained that the real purpose of the bill was the creation of a partnership with the private sector to protect the U.S. in case of a significant cyberattack over the critical infrastructure. This partnership became critical mainly because, according to the U.S. government, DHS was not very active preventing actions when cyberattacks occur (U.S. Senate, 2010e). Senator Rockefeller also claimed how dangerous the Internet could be:

Author: Former Senator John Rockefeller (U.S.), 2009 About Bill S.773	*About bill S.773:* "President Obama's chief of national intelligence, admiral Blair to whom I respect, have labeled cyber security perpetrated through the Internet as the number one national hazard of attack in West Virginia, in America, in anywhere else … It really make to ask you the question whether it was better for you never invented the Internet …" (DarkvanM, 0:50, 2009) "Everybody is attacked, anyone can do it…" (DarkvanM, 2009, 1:40) "it is an act that shut this country down …" (DarkvanM, 2009, 2:05) "[Bill S.773] … builds on the idea that cyber security is a shared responsibility between the public and private sectors, that's what this whole bill is about," (Walker, 2010, para.3) "We are recognizing that traditional regulation will not work because a bureaucracy simply cannot keep up with the necessary pace of invention. Likewise, it should be clear that leaving our security solely to the market is also a failing strategy. Neither approach can combat the threats that we face alone and together," (Walker, 2010b, para.6)

[24] "S.773.- Cybersecurity Act of 2009"
Sec. 18. Cyber security responsibilities and authorities.
"The President— "
….
"(2) may declare a cyber security emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network;"
…
"(6) may order the disconnection of any Federal Government or United States critical infrastructure information systems or networks in the interest of national security;"

> "We want the private sector to take a lead. It's very much the time to give the private sector the tools it needs to collaborate with the government and address this monumental challenge." (Walker, 2010b, para.7)

Senator Rockefeller and sponsors of the bill prepared a report where they explained the necessity of the partnership they proposed with the private sector (Senate Report 111-384) to the Committee on Commerce, Science and Transportation from the U.S. Senate. These were their views:

> "If we [the U.S.] went to war today in a cyberwar, we would lose. We're the most vulnerable, we're the most connected, we have the most to lose."\1\ Public and private sector computer networks within the U.S. are increasingly subject to attack." (U.S. Senate, 2010d, para.5)

> "The private sector owns a large percentage of the nation's critical infrastructure, including electricity generation and transmission, water and sewer treatment facilities, and financial markets and clearinghouses. The computers that run these systems are often interconnected and subject to the same potential attacks as other networks. Experts suggest that cyberattacks against critical infrastructure potentially could physically destroy infrastructure, depriving large populations of essential goods and services for extended periods of time and threatening lives." (U.S. Senate, 2010d, para.5)

> "… a number of reports demonstrate that DHS has not been fully effective in improving cyber security throughout …" (U.S. Senate, 2010d, para.7)

> "The primary goal of the Cybersecurity Act of 2010 is to modernize the public-private sector relationship on cybersecurity. As a vast majority of our Nation's networks are owned and operated by the private sector, securing cyberspace must be a collaborative effort between our Government and the private sector." (U.S. Senate, 2010d, para.18)

The private sector strongly opposed to bill S.773 because it was not clear what type of authority the government would have over the private sector (McCullagh, 2009). The U.S. Senate never passed S.773 (GPO, 2010), but the Internet shutdown debate did not stop there. In 2010, Senator Lieberman and sponsors introduced bill S.3480 to the Committee on Homeland Security of the U.S. Senate. Differently, from bill S.773, S.3480 did not include a paragraph that would

grant powers to the president to shut down the Internet. Nevertheless, both bills raised similar concern because this new legislation would force companies such as ISPs, search engines, or software firms to comply with any emergency measure or action developed by DHS. The purpose of the new bill was the preservation of the critical infrastructure (McCullagh, 2011a).

The bill proposed (with the support of DHS) the creation of a National Center for Cybersecurity and Communications (NCCC). NCCC shall be headed by a Director, who shall work cooperatively with the private sector to secure, protect, and ensure the resiliency of the federal and national information infrastructure (Senator Lieberman, 2011b).

Like it happened with S.773, sponsors and supporters of bill S.3480 also had the intention to build a partnership with the private sector to protect the U.S. critical infrastructure from a major cyber-attack:

Author: Former Representative for California's 36th congressional district Jane Harman (U.S.), 2010	*About bill S.3480:* " … we face daunting challenges in tackling this problem, including: a lack of sustained leadership, insufficient resources, authority to enforce actions in the event of an imminent cyber attack, the need to partner with other federal agencies and private sector entities and insufficient education and training" (Harman, p.E1123, 2010) "… it would create a National Center for Cybersecurity and Communications at the Department of Homeland Security to identify and mitigate cyber vulnerabilities. The Center would be charged with providing situational awareness, conducting risk-based assessments of threats, identifying vulnerabilities, managing external access points for federal networks, overseeing operations of US-CERT, and working with the private sector to establish security requirements to strengthen vital components of critical infrastructure like the electric grid and telecommunications networks" (Harman, p.E1123, 2010)
Author: Former Senator Joseph	*About bill S.3480:* "As we have seen repeatedly, from the financial crisis to the environmental catastrophe in the Gulf of Mexico, what happens in the

Lieberman (U.S.), 2010	private sector does not always affect just the private sector. The ramifications for government and for the taxpayers often are enormous. This bill would establish a public/private partnership to improve cyber security. Working collaboratively with the private sector, the Center would produce and share useful warning, analysis, and threat information with the private sector, other Federal agencies, international partners, and state and local governments. By developing and promoting best practices and providing voluntary technical assistance to the private sector, the Center would improve cyber security across the nation. Best practices developed by the Center would be based on collaboration and information sharing with the private sector. Information shared with the Center by the private sector would be protected" (U.S. Senate, p.S4854, 2010c)

Additionally, Senator Lieberman and the other sponsors of the bill prepared a report (U.S. Senate, 2010d) to the Committee on Homeland Security and Governmental Affairs from the U.S. Senate. Their views on the private sector are the following ones:

> "The private sector owns a large percentage of the nation's critical infrastructure, including electricity generation and transmission, water and sewer treatment facilities, and financial markets and clearinghouses. The computers that run these systems are often interconnected and subject to the same potential attacks as other networks. Experts suggest that cyberattacks against critical infrastructure potentially could physically destroy infrastructure, depriving large populations of essential goods and services for extended periods of time and threatening lives" (U.S. Senate, para.9, 2010)

> "The primary goal of the Cyber Security Act of 2010 is to modernize the public-private sector relationship on cyber security. As a vast majority of our Nation's networks are owned and operated by the private sector, securing cyberspace must be a collaborative effort between our Government and the private sector" (U.S. Senate, para.13, 2010).

Regarding bill S.3480 there is one statement that was never mentioned. Back in 2010, Senator Lieberman, while referring to an Internet shut down and attacks over the critical infrastructure, he made the following statement:

> "… And we need this capacity in a time of war. We need the capacity for the president to say, Internet service provider, we've got to disconnect the American Internet from all traffic

> coming in from another foreign country, or we've got to put a patch on this part of it" (CNN, 2010, para.53)
>
> "Right now, China, the government, can disconnect parts of its Internet in a case of war. We need to have that here, too." (CNN, 2010, para.53)

These comments made clear that ISPs play an important when it comes to stopping Internet access. Additionally, comments about China were not welcome for the civil society in the U.S. because, back in 2010, China use this extreme policy to silence the political rivals of the ruling party exclusively (MacKinnon, 2012). Although Senator Lieberman made very clear that his intention with S.3480 was not attacking the freedom of speech or the free flow of information, it is not clear what he intended by mentioning the Chinese use of an Internet shut down.

The last bill to analyze is S.413. This time Senator Lieberman and his co-sponsors of the bill[25] took the precaution of adding a provision that forbids the president, the Director of the National Center for Cybersecurity and Communications (NCCC Director) or any other federal employee to shut down the Internet[26]. Nevertheless, the bill was still criticized because of the potential contradiction among its provisions and the lack of clarity about the powers of the NCCC

---

[25] Cosponsors of the bill include:
Collins, Susan M. [R-ME]* (joined 02/17/2011)
Carper, Thomas R. [D-DE]* (joined 02/17/2011)

[26] "S.413.- Cybersecurity And Internet Freedom Act of 2011"
SEC. 2. INTERNET FREEDOM ACT.
(a) Short Title. —This section may be cited as the "Internet Freedom Act".
(b) Findings. —Congress finds that—
…
(4) the Internet has developed into a robust network within the United States, with thousands of providers, making it technically impossible to shut down the Internet;
…
(10) neither the President, the Director of the National Center for Cybersecurity and Communications, nor any other officer or employee of the Federal Government should have the authority to shut down the Internet.
(c) Limitation. —Notwithstanding any provision of this Act, an amendment made by this Act, or section 706 of the Communications Act of 1934 (47 U.S.C. 606), neither the President, the Director of the National Center for Cybersecurity and Communications, or any officer or employee of the United States Government shall have the authority to shut down the Internet."

Director[27]. The latter one would be able to decide what owners and operators of the critical infrastructure must do if a national emergency is declared. The NCCC Director had authority to determine on this. For this reason, this bill also identified the private sector that owns and handles the critical infrastructure as the audience to convince if shutting down the Internet was necessary:

Author: Senator Thomas Carper (U.S.), 2011	*About bill S.413:* "All aspects of American society have become increasingly dependent on the internet whether we're talking about the military, the government, or businesses both small and large. While in most cases this powerful technology has transformed our daily life for the better, unfortunately bad actors – from common criminals to foreign terrorists-- have identified cyber space as an ideal 21st century battlefield. We have to take steps now to modernize our approach to protecting this valuable, but vulnerable, resource. We also have to balance our need for security in this new frontier with our democratic values of freedom and liberty. This legislation strikes that careful balance – providing the tools that America needs to better protect cyber space while additionally protecting our civil liberties. It encourages the government and the private sector to work together to address this growing threat and provides the resources for America to be successful in this critical effort." (Senator Carper, para.7, 2011)

[27] "S.413.- Cybersecurity And Internet Freedom Act of 2011"
"SEC. 249. NATIONAL CYBER EMERGENCIES.
"(a) Declaration. —
….
"(3) AUTHORITIES. —If the President issues a declaration under paragraph (1), the Director shall—
"(A) immediately direct the owners and operators of covered critical infrastructure subject to the declaration under paragraph (1) to implement response plans required under section 248(b)(2)(C);
"(B) develop and coordinate emergency measures or actions necessary to preserve the reliable operation, and mitigate or remediate the consequences of the potential disruption, of covered critical infrastructure;
"(C) ensure that emergency measures or actions directed under this section represent the least disruptive means feasible to the operations of the covered critical infrastructure and to the national information infrastructure;
"(D) subject to subsection (g), direct actions by other Federal agencies to respond to the national cyber emergency;
"(E) coordinate with officials of State and local governments, international partners of the United States, owners and operators of covered critical infrastructure specified in the declaration, and other relevant private section entities to respond to the national cyber emergency;
…"

Moreover, during a hearing before the subcommittee on cybersecurity infrastructure protection, and security technologies, the House of Representatives, concluded that the private sector model of action would act faster while facing a cyberattack:

> "Congress must make a realistic assessment as to whether an information- sharing model that puts the Government at the center—receiving information, analyzing it, and sharing the resulting analysis with industry—could ever act quickly enough to respond to fast-moving threats. Though the White House cybersecurity proposal 7 and the lead Senate bill, the Cybersecurity and Internet Freedom Act, (S. 413) adopt the Government-centric approach, we have serious concerns about it. An industry-based model, subject to strong privacy protections, would be able to act more quickly and would raise few, if any, of the Fourth Amendment concerns associated with a Government-centric model" (Subcommittee on Cybersecurity, p.22, 2011)

The White House cybersecurity initiative of 2011 contains a similar approach about the private sector:

Statement for the Record of Philip Reitinger, Deputy Under Secretary National Protection, and Programs Directorate, DHS and others	*About the White House Proposal: Cybersecurity Regulatory Framework for Covered Critical Infrastructure:* "Sensitive information is routinely stolen from both government and private sector networks, undermining confidence in our information systems, the information collection and sharing process, and the information these systems contain" (Phillip Reitinger et al., 2011, para.5)

I conclude that the audience for all the Internet shutdown bills in the U.S. is the private sector, the private sector that owns and handles the critical infrastructure and the Internet infrastructure. The situation here is very similar to the Australian case: (1) The private sector owns and controls the critical infrastructure, (2) The private sector owns and manages the Internet infrastructure and (3) There is a failure of national security agencies to work in a partnership with the private sector. These are the reasons why a partnership with the private sector is a recurrent element among these three bills and the White House proposal. An Internet shutdown cannot be

accomplished without the private sector, and at the same time, the private sector needs to agree because they own and handle the critical infrastructure, so vital for the U.S. The private sector not only holds and operates the majority of the critical infrastructure, these companies are also able to reach networks the U.S. government cannot (Germano, 2014).

Finally, the last case is the U.K. Back in 2011, after the Egyptian Internet shutdown, representatives of the U.K. government analyzed the possibility of shutting down the Internet in that nation-state. Specifically, representatives of the U.K. Department for Culture, Media and Sport agree on the possibility under the following terms:

Author: Representatives of the Department for Culture, Media and Sport (U.K.), 2011	*Responding a question about the possibility of shutting down the Internet in U.K. territory:* "It would have to be a very serious threat for these powers to be used, something like a major cyber attack. The powers are subject to review and if it was used inappropriately there could be an appeal to the competitions appeal tribunal. Any decision to use them would have to comply with public law and the Human Rights Act" (Hardings, 2011).

The U.K. government officials put emphasis on the balance between freedom of information and protection of the public, although there is no major explanation of what that means. From the statement of the representative of the Department for Culture, Media and Sport, the arguments in favor of an Internet shut down would be: 1. The presence of a severe threat and 2. An example of that threat is a significant cyberattack, but it is not the only case. Within the same context, it is necessary to look at the statements of British representatives about the cyber security policy of the U.K. back in 2011:

Former Minister of State for the Armed	*Speech in the KOKODA Foundation, Queensland, Australia:*

Forces Sir Nick Harvey (U.K.), 2011	"The private sector has to lead in the development of improved Internet security products, systems, services and standards in cyberspace" (Harvey, 2011)

The U.K. cyber security policy (from 2011) itself was also very explicit about the private sector role:

> ".... working in partnership...
> 3.3 Though the scale of the challenge requires strong national leadership, Government cannot act alone. It must recognise the limits of its competence in cyberspace. Much of the infrastructure we need to protect is owned and operated by the private sector. The expertise and innovation required to keep pace with the threat will be business-driven" (Cabinet Office, p.6, 2011)

The new cybersecurity policy of the U.K. government, published in November 2016, reinforced the role of the private sector as the one that owns and manages the critical infrastructure of that nation-state:

> "The cyber security of certain UK organisations is of particular importance because a successful cyber attack on them would have the severest impact on the country's national security. This impact could have a bearing on the lives of UK citizens, the stability and strength of the UK economy, or the UK's international standing and reputation. This premium group of companies and organisations within the public and private sector includes the critical national infrastructure (CNI), which provides essential services to the nation. Ensuring the CNI is secure and resilient against cyber attack will be a priority for the Government …" (HM Government, 2016, p.40)

The new U.K. cybersecurity strategy also includes those who interact with the ones who own and handle the critical infrastructure in that nation-state to address and prevent the risk they may face:

> "… we will work through organisations such as insurers, regulators and investors which can exert influence over companies to ensure they manage cyber risk" (HM Government, 2016, p.23)

So far, similarities between the U.S. and U.K. discourses are undeniable. According to their securitizing agents, a significant cyberattack over the critical infrastructure could prompt an Internet shutdown, one that cannot be achieved without the collaboration of the private sector. Within this context, the private sector becomes the primary audience: (1) The private sector owns and handles the critical infrastructure and (2) The private sector owns and handles the Internet and the telecomm infrastructure (which is at the same time part of the critical infrastructure) to try to achieve an Internet shutdown if the case demands it. The securitizing agents, government legislators, expect the backup of the owners of the critical infrastructure and the collaboration of the owners of the Internet infrastructure. Without the participation of the latter ones, the extreme measure the securitizing agents want to concretize, an Internet shutdown, cannot be accomplished. On this point, as mentioned before, Senator Lieberman would consider commanding ISPs, as part of the first step to shutting down the Internet:

> " … We need the capacity for the president to say, Internet service provider, we've got to disconnect the American Internet from all traffic coming in from another foreign country…" (CNN, 2010, para.53)

In this way, similarly to the Australian case, ISPs also became the first actors of the chain being instrumental in the protection of the critical infrastructure. Nevertheless, it is important to clarify that ISPs are not the audience, but some of the operators to grant Internet access to the Internet users.

Additionally, and differently from the U.S. and Australia, the U.K. speech has a difference. The first time the U.K. government addressed the possibility of shutting down the Internet was during the riots of 2011 when Prime Minister Cameron blamed the social networks, like Facebook, Twitter and the old Blackberry message system of expanding violence (Nosowitz, 2011).

The riots in London took place between 6 and 11 August 2011. The riots were the outcome of cuts into the national budget by a new government (a Conservative and Liberal Democrat coalition), rises in tuition fees and the killing of one man by the police in a local black community (Suleyman, 2017). For five days buildings and vehicles were smashed and get on fired, while stores were looted. The police deployed around 16,000 police officers in London's streets to try to stop the violence (Alan Taylor, 2011). Back in those days, British newspapers claimed that the riots were "fueled by social media" (Halliday, 2011, para.4). Scotland Yard warned about those calling for violence episodes on the "140-character social network would not go unpunished" (Halliday, 2011, para.9). However, the fastest and accurate tool was a more covert social network: BlackBerry Messenger (BBM). Unlike Twitter and Facebook, authorities could not trace BBM (Halliday, 2011a). Nevertheless, for the police any tool they could to track protesters was worthy. The police warned of incitement to violence after a campaign on Facebook, BBM, and Twitter (Douglas, 2011).

As mentioned before in this dissertation, although Prime Minister Cameron's public message was that the government wanted a master switch to shut down the social networks, his initial intention was shutting down the entire Internet. The British government dismissed this option because of the possible impact in the international community who could compare the British decision with the Egyptian case (DH, 2011; Ghosh, 2011; Marsden, 2011; Williams, 2011).

In any case, Mr. Cameron was very clear blaming the social networks for the riots and questioned the use of the free flow of information. At the time, he offered to the police all the resources they may need to track episodes they considered plots for violence in the social networks:

Former Prime Minister David Cameron (U.K.), 2011	*Mr. Cameron's statement to the House of Commons about the 2011 riots:* "So we are working with the Police, the intelligence services and industry to look at whether it would be right to stop people communicating via these websites and services when we know they are plotting violence, disorder and criminality" …" (Cameron, para.63, 2011a)

Following the riots, Mr. Cameron called for a crackdown on social media, while Mr. Nicolás Sarkozy (President of France back in 2011) called for a "civilized Internet" (NDTV, 2011). Mr. Cameron also informed that Theresa May, at the time Home Secretary, would hold meetings with Facebook, Twitter, and Research In Motion to discuss their responsibilities in cases like this (Halliday, 2011b).

In this last case, the audience to whom governments of consolidated democracies address when implementing cyber security policies related to an Internet shutdown is indeed the private sector, but not the one that controls and handles the critical infrastructure. Within the private sector, there are different audiences: (1) the one that owns and manages the critical infrastructure, (2) the one that facilitates the free flow of information – in particular, the one that owns and operates the social networks' platforms or massive communication means-. The case of the riots in London is a case where the government wants to interfere in the free flow of information for social control purposes, or as the British government stated, to keep the public order under control. Mr. Cameron referred it is a case where free flow of information is "used for ill" (Cameron, 2011a, para.63).

In this case, social media platforms are not instrumental in shutting down the Internet. This audience fulfills a different role. As explained previously, although actions of audiences may vary across cases, audiences do have the potential to exert influence over securitization processes and the policies selected to address potential threats (Côté, 2016).

The goal of the U.K. government was to stop the riots from 2011, an action with purposes of social control. To accomplish such mission, it was necessary to control the flow of information that allowed spreading the violence through the social networks. In this scenario, social network platforms are directly instrumental in controlling the flow of information. For a government, the most common way to control such mechanisms of social participation is using disruptive policies to regulate the Internet infrastructure, being censorship the most common one. Censorship also can escalate to attempt to shut down the entire Internet; such decision usually belongs to the securitizing agent depending on the circumstances (Dunn, 2011; MacKinnon, 2012; Mejias, 2013). In the British case, the speed of the events during the riots prompted the U.K. government to consider shutting down the Internet. If such policy was not finally applied (and nor was a censorship policy) was because of the international context that could compare the U.K. with the Egyptian Internet shutdown (Williams, 2011).

In this case, social network platforms, voluntarily or not, influenced the securitization processes and the policies considered by the U.K. government to address a potential threat against the social order. U.K. authorities saw an Internet shutdown as the way to stop the flow of information when that nation-state was facing violent events. In this way, although not instrumental to shut down the Internet, social platforms did influence the security speech of the U.K. government that considered an Internet shutdown.

4.3.3.1.2. Hybrid Regimes

Although Russian claims overt the Internet started between 2003 and 2005 during the World Summit on the Information Society (WSIS), these claims became stronger after the Snowden revelations in 2013 (Jr., Lawson, & McFarlane, 2015; WSIS, 2015).

In general, hybrid regimes became eager to protect the flow of data within their territories and their national Internet infrastructures. Some academics call this government tendency "cybernationalism". Although Brazil (a young democracy) was portrayed as the main creator of this new tendency, it would be hybrid regimes the ones who took it to the extreme (Costello, 2017; Keating, 2013b; Messmer, 2013). After 2013, the Russian government created a group of laws with the purpose of "align" RuNet with this idea of cybernationalism by (1) forcing operators of websites to store all information they process and keep it available to be reviewed by Russian authorities when required, (2) holding censoring attributions for the Russian regulator at its own discretion, and (3) forcing private companies to store data within servers located in Russian territory (Duffy, 2015).

As consequence of these new laws, the private sector became very critical against Vladimir Putin's administration. Russian bloggers and Internet experts expressed their concern that this new set of security policies may be an attempt to restrict freedom and isolate Russia from the global network (Zavyalova, 2014).

In the middle of this situation, Culture Minister Vladimir Medinsky and deputy Prime Minister Dmitry Rogozin were among the signatories to a statement by the Russian Military Historical Society where they warned about a "new blitzkrieg" against Russia – "and thus against the truth" (Demirjian, para.1, 2015). Both officials referred to the creation of a "Patriotic Internet" that can protect Russian citizens from the U.S. espionage activities (Dolgov, 2015a). In this regard,

Russian authorities spoke about the "unpredictable west" that can "disconnect" the Russian Internet from the global Internet and compromise the integrity of the Internet itself and the personal data of Russian citizens (Belousov, 2014):

Former communications minister Igor Shchegolev and aide to President Vladimir Putin (Russia), 2014	"the actions of our partners in the United States and Europe have recently acquired a certain degree of unpredictability and we should be prepared for this" (Belousov, 2014)
Presidential press secretary Dmitry Peskov (Russia), 2014	"It is common knowledge who the main administrator of the global internet is. Given this unpredictability, we must think of how to ensure our national security" (Zavyalova, 2014).

As well pointed out by some cybersecurity experts in Russia, the target of the latest laws (but not the audience) over RuNet is the social network platforms originating from abroad, such like Facebook and Twitter. These companies handle the flow of information at a world level and Russians citizens' private data and Russian government data, in a way that Russian authorities cannot control. The government new laws enacted in September 2014 also targeted cyber activism, bloggers and market players (Hille, 2015; Zavyalova, 2014).

The new laws required all online companies to store Internet users' personal data within Russian territory and was expected to be in force by September 2016, but the date was later rescheduled to January 2015 (Eremenko, 2014a; Koshkin, 2014). The preamble of the law stated that it was created to "ensure the protection of Russian citizens' rights to telecommunication privacy and personal data safety" (Eremenko, 2014, para.3). In this regard, Russia's Oversight Communication Agency (Roskomnadzor) warned Google, Facebook, and Twitter that they must

be registered as “organizers of information distribution” in compliance with the law (Koshkin, 2014).

The Russian scenario shows that social networks are the targets of an aggressive policy to force them to keep the data they handle within Russian territory. In those circumstances, the key point in this debate is the data, who owns it and how to control it (Hille, 2015; RT, 2013b, 2014a).

The importance of the data is such that, for Russian authorities, a foreign attack that can trigger an Internet shut down is an attack from a foreign power (most likely the U.S.) that: 1) would make the Russian government to lose control over its own data and its citizens’ and that 2) would make the Russian government to lose control over the Internet infrastructure. The fear of Russian authorities exists because social networks control data that the government cannot access and cannot control (Galperina, 2016; Lunden, 2016; The Washington Post & Reuters, 2016).

According the Russian perspective, these two scenarios are only possible because of the actions of private companies based in the U.S. that handle Russian data, such as Google, Facebook, Twitter and LinkedIn. When considering an Internet shutdown, Russian authorities think in the flow of information, in this way the situation turns at some extent, very similar to the one in the U.K. Social networks are not instrumental to achieve an Internet shutdown, but they are the receivers of the security discourse and take a role in its creation. Depending upon their positive or negative response towards governments’ policies, the government will involve the owners and operators of the Internet and telecom infrastructure in achieving an Internet shutdown. Just like in well-consolidated democracies, the private owners of the Internet and telecom infrastructure are the ones that formed the audience. If the ones in charge of the data flow don’t cooperate with the Russian government, then the turn to act will be for the owners and operators of the Internet and telecom infrastructure. That is the audience the Russian government needs to convince.

When considering specifically an Internet shutdown, Russian authorities stated that, it is not their intention to disconnect the Internet, but they must be prepared for potential unpredictable actions of the west. Following this line of action, on October 1, 2014, the Russian Security Council discussed the possibility of shutting down the Internet as an emergency procedure if there are circumstances of national security. In that scenario ISPs should be habilitated to stop their services if required by the government (Belousov, 2014; Harding, 2014; Kramer, 2014a; MacAskill, 2014; Watson, 2013). ISPs are just some of the actors within the Internet ecosystem. They just play a role as part of the audience, but they are not the audience. The audience as a whole is the owners and operators of the Internet infrastructure within Russian territory, in particular the private ones.

As mentioned before, an Internet shut down is acceptable under two circumstances: (1) if it is ordered by Russian authorities and (2) if it helps to preserve the control the Russian government has over the infrastructure of RuNet, the government's data and its citizens' data (AFP, 2014; Bodner, 2014; Kramer, 2014b). Facing this context ISPs must be ready to act according the commands of the government and foreign companies were required to store all Russian data in servers within Russian territory. According to the government provisions, Russian ISPs will be required to make possible to shut down Russia's Internet access to the global Internet during military actions or serious protest actions (Stone, 2014b). By statement of the representatives of the State Duma (Госуда́рственная Ду́ма), the Internet could not remain as a space free of regulation, like it was before the Snowden revelations (DUMA, 2014).

Leonid Levin, Chairman of the State Duma Committee on Information Policy, Information Technology and	"For many years, we lived in a completely free and legal regulation of the Internet procedures, it seemed to many that the Internet - is a free zone, without the participation of the state. The inertia of such sentiment was not entirely been eliminated even as a result of revelations Snowden, and in fact they clearly showed that the Internet in bad faith are not only organized hooligan and criminal groups of

Communications (2014)	hackers, but also the most developed nations of the world on the Internet are no less hard than in other spheres, and our country must be ready for it. State hacking is not only capable of destroying private life or business of the individual citizen, but may well be a real threat to the freedom and independence of our country, is a good example of this - the situation with the protection of personal data: on foreign servers personal information of Russian citizens are not protected, subjected to illegal collection and use. If this was done only for marketing purposes, and in a few cases, a network of hooliganism, it might have been at least some reason to say that it costs the power of freedom, however, as is conclusively proved Snowden its revelations, personal data researched by foreign state structures that are highly likely doing it for use against the interests of the Russian Federation, in violation of the security of Russian citizens" (DUMA, para.45, 2014).
Nikolai Anatolyevich Nikiforov, Minister of Communications and Mass Media, (Russia), 2015	Authorities were to begin testing various methods "to prevent Russia being cut off from the Internet from abroad" (Bernard, para.2, 2015) "We modeled what would happen if our respected foreign partners, under the influence of the latest mood of their politicians who play with sanctions, suddenly decide to take this or that measure against Russia," (Bernard, para.4, 2015) "Our task is to do what is needed so that the Russian Internet will carry on working independently of the opinion of colleagues, whatever sanctions policy decisions they decide to take." (Bernard, para.4, 2015)

In March 2018, Vladimir Putin's Internet adviser German Klimenko sought to reassure Russians that contingency plans are ready in case RUNET is disconnected from the global Internet. While offering an interview about hypothetical Internet shutdown Klimenko stated that "If our colleagues disconnect us from the switch tomorrow, I don't know if it will be painless, though we've been promised that it will be painless," (The Moscow Times, 2018, para.3).

Before these statements, in 2014, President Vladimir Putin called the Internet a "CIA project," created with the purpose of weaken Russia's government and punish that nation-state finally. Mr. Putin also claimed that Russia needed to be protected from the Internet and that his

administration has a duty to resist foreign influence and fight for its interests online (MacAskill, 2014).

At the beginning of 2014, Minister Yevgeny Fyodorov warned that Russia would face a period of aggression, and therefore, they should be prepared, and its defenses should include mass media and information. Fyodorov also advocated for the transference of all data stored in Russia to the hands of Russian specialists appointed by the government. In this context, Fyodorov accused Google of taking "an openly anti-Russian position" (RT, para.5, 2014a) and of signing a cooperation agreement with the Ukrainian special services in order to transfer Russian citizens' personal data. Additionally, Senator Lyudmila Bokova accused Google of violating the national law on personal data by scanning users' content, including emails. The position against Google was so extreme that after the Snowden revelations, several Russian MP suggested that the government should change the contracts of civil servants and forbid them of using Google and social networks that store in the U.S. (Reuters, 2014, 2015, RT, 2014b, 2014d).

MP Yevgeny Fyodorov Chairman of the factional groups in the State Duma of the Russian Federation (2014)	"We hold that in due time we must see the nationalization of Google, meaning that Google's operations concerning Russia must fall under Russian jurisdiction and competence" (RT, 2014b)
MP Yevgeny Fyodorov Chairman of the factional groups in the State Duma of the Russian Federation (2014)	"Google remains in the jurisdiction of the United States of America and the USA is now officially seeking to weaken Russia and destabilize the situation. This is a direct order for all organizations that fall under its control," (RT, 2014d)

According to the statement of Russian policymakers the audience of the Russian government is focus in two actors: private corporations based abroad (like Google and social network platforms) that handle the flow of data in and out of Russian territory and the owners (and the ones who handle) the Russian telecomm infrastructure and Internet infrastructure. The first ones are the receivers of the speech and depending upon their response the latter ones must act. The Russian speech points to a great fear of losing control of the data of their citizens and the government itself and, fear of losing control of the national Internet infrastructure.

The called Blitzkrieg laws of the Russian government have increased the control the Russian government has over the different members of the Internet ecosystem located in Russian territory. Just to point an example, Russia may not have a unique government-owned ISP, but they do have a set of tools and laws to control private ISPs. This is a common characteristic with Venezuela, another hybrid regime under study. The Russia approach intends to keep their citizens' data in servers located within their own territory, so rival nation-states cannot have access to their communications.

The Russian position is the case of a hybrid regime, but it is not the only one. The Venezuelan case is slightly different from the Russian one. The audience is also focus in social media, but for different reasons from the Russian case. As a matter of fact, the concern of the Venezuelan government over the Internet began a few years before the world knew about the Snowden revelations in 2013. In 2010 the former Venezuelan President Hugo Chavez claimed that "la Internet no puede ser una cosa libre" ["the Internet cannot be a free thing"] (cadsvm, 2010, 4:35) because the flow of information may be false and there is no way to control it. Chavez made this statement while blaming the digital platform of "Noticiero Digital" ["Digital News"] of

allowing individual citizens to post whatever they want in its webpage (cadsvm, 2010; MrBarbacoa2011, 2010; Perfil Internacional, 2010).

Former Venezuelan President Hugo Chavez (2010)	"The Internet cannot be something open where anything is said and done. Every country has to apply its own rules and norms" (Chinea & Daniel, 2010, para.2)
Former Venezuelan President Hugo Chavez (2010)	"We have to act. We are going to ask the attorney general for help, because this is a crime. I have information that this page periodically publishes stories calling for a coup d'etat. That cannot be permitted" (Chinea & Daniel, 2010, para.4; El Pais, 2010)

Following this statement, the Venezuelan government included the Internet in the "Ley de Responsabilidad Social y Calidad de Television" ["Law of Social Responsibility and Quality of the Television"], also known as RESORTE. According to this law, the Venezuelan regulator (CONATEL) can decide when the content published is illegal according the circumstances included in the law itself and the executive branch may decide the punishment for the violator. This law also established responsibility for third parties, in particular ISPs and social network platforms, as they are directly involved in the data management process (Finol & Espinoza, 2015; Gonzalo, 2010)[28].

[28] Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos
Capítulo VI. - Del Fondo de Responsabilidad Social y de las Tasas
Artículo 27
Prohibiciones
En los servicios de radio, televisión y medios electrónicos, no está permitida la difusión de los mensajes que:
1. Inciten o promuevan el odio y la intolerancia por razones religiosas, políticas, por diferencia de género, por racismo o xenofobia. 2. Inciten o promuevan y/o hagan apología al delito. 3. Constituyan propaganda de guerra. 4. Fomenten zozobra en la ciudadanía o alteren el orden público. 5. Desconozcan a las autoridades legítimamente constituidas. 6. Induzcan al homicidio. 7. Inciten o promuevan el incumplimiento del ordenamiento jurídico vigente.
…
Los proveedores de medios electrónicos serán responsables por la información y contenidos prohibidos a que hace referencia el presente artículo, en aquellos casos que hayan originado la transmisión, modificado los datos, seleccionado a los destinatarios o no hayan limitado el acceso a los mismos, en atención al requerimiento efectuado por los órganos con competencia en la materia.

Translation:

Law of Social Responsibility in Radio, Television and Electronic Media

Differently from Russia, the Venezuelan government did shut down the Internet. As previously mentioned, the first time was in April 2013, during the Presidential elections after former President Hugo Chavez died. Back then, Jorge Arreaza (then vice-President) claimed that foreign hackers attacked the Twitter accounts of the Venezuelan ruling party, "Partido Socialista Unido" – PSUV [United Socialist Party of Venezuela], the candidate Nicolás Maduro (at the time also interim president and today's president) and the webpage of the Consejo Nacional Electoral – CNE [National Electoral Council] (AVN/VTV, 2013).

Former Venezuelan Vice President and Minister of Science and Technology Jorge Arreaza (2013)	"Un grupo de hackeadores del exterior anuncia un posible hackeo a la página del CNE. Inmediatamente se hacen las coordinaciones con el CNE, y para proteger la página se decide impedir que tenga acceso desde el exterior; el acceso se deja nacional. Cualquier venezolano entrará en la página web del CNE después que se dé el boletín y tendrá acceso a los resultados electorales. Bueno, desde el momento el que se tomo la decisión de bloquear desde el exterior hasta este momento han habido 45,000 intentos, lo que pasa es q están bloqueadas esas páginas. Si no hubiésemos hecho lo que hicimos, esa página estaría caída porque es un hackeo que no sabemos decir de dónde. Sabemos que no es de Venezuela, a veces ellos se disfrazan con distintos códigos, a veces desde Estados Unidos, a veces desde Europa. Ahora en el momento en el cual nosotros hicimos los trámites para impedir que desde el exterior se tenga acceso a los 4 servidores del CNE, que es lo único que se hizo, se produjo en la sintaxis en las palabras, una caída de la Internet que no duro más de tres minutos, casi cuatro minutos en realidad, para ser sincero" (Bracci Roa,0:41,2013; noticias24, 2013)

Chapter VI.- About the Social Responsibility Fund and Fees
Article 27
Prohibitions
In the radio, television and electronic media services, the dissemination of messages that:
1. Encourage or promote hatred and intolerance for religious, political, gender, racist or xenophobic reasons. 2. Encourage or promote and / or advocate for crime. 3. Make propaganda for war. 4. Encourage disorder among the population or disturb the public order. 5. Do not recognize the legitimately constituted authorities. 6. Induce homicide. 7. Encourage or promote breach of the current legal system.
...
Electronic media providers will be responsible for the prohibited information and content previously mentioned in this article, in those cases that they were responsible for originating the transmission, modified the data, selected the recipients or did not limit access to them, in spite of the request made by the competent authorities.

> "Alerta que la cuenta de @NicolásMaduro ha sido hackeada! ¡Sus últimos mensajes son falsos!" (Venprensa, 2013)
>
> *Translation:*
>
> "A group of foreign hackers announced an attack to the CNE webpage. Immediately we coordinated with CNE, and in order to protect the webpage it was decided to stop all access from abroad; national access was allowed. Any Venezuelan will be able to access the CNE webpage after the bulletin and will have access to the electoral results.
> Well, since the moment we took the decision of blocking from foreign countries until this moment there were 45,000 attempts, but those pages are blocked. Had us not done what we did, that page would be affected because it is a hacking that we don't know where it comes from. We know it is not from Venezuela, sometimes they disguise with different codes, sometimes from the United States, sometimes from Europe. Now, in the moment we act to stop the attack over the CNE four servers, which was the only action, an Internet shut down took place, which did not take more than three minutes, almost four, to be honest"
>
> "Alert the account of @NicolásMaduro has been hacked! His last messages are false"

The CNE is the government agency in charge of counting electoral votes and by constitutional mandate it should be independent from any other government institution. However, the CNE impartiality and neutrality was questioned during the 2013 elections and is constantly used as a communication platform by the government (Barboza Gutiérrez, 2012, 2014; Nuñez & Ochoa, 2013). According to Mr. Arreaza, to protect the CNE webpage, the social platforms of the ruling party (Twitter specifically) and its candidate and public agencies website from foreign cyberattacks, the Venezuelan government decided to shut down the Internet, so foreign nation-states could not have any access. This process took around four minutes in Caracas (the capital city) and between 20-45 minutes in the rest of the Venezuelan territory. This Internet shutdown was highly successful because the government owns CANTV, the ISP that handles over 90% of

the Internet subscribers in Venezuela (Bracci Roa, 2013; Diaz Hernandez, 2013; Venprensa, 2013).

Political rivals accused Mr. Arreaza and the ruling party of taking these actions to manipulate the electoral data. Mr. Arreaza rejected the accusations stating that there was no problem with the Internet and that they were just trying to protect the sites previously mentioned from foreign attacks. In this case, the foreign attack has a different connotation from the Russian one. According the statement of its own representatives, the government was trying to protect the communication platforms of the ruling party, which include Twitter accounts and official web pages. Venezuelan authorities claimed that attackers were foreigners living outside of Venezuelan territory, although this was never clarified (OpenNet, 2013).

Venezuela has lived many episodes of censorship in the past and they continue, but this was the first time the Internet was shut down (OpenNet, 2013; Reuters, 2017b). This episode was not related to the flow of data or information, but to the communications capabilities of the ruling party in times when its stability in power was not clear. At this point it is necessary to remember that one of the reasons why Venezuela is considered a hybrid regime is because the same party has been ruling since 1999 (EIU, 2017). The Venezuelan authorities at the time and even today use their Twitter accounts and public agencies websites, the CNE in particular, as part of their communication infrastructure or platform to address the rest of the world. As a matter of fact, the CNE has been accused many times of lack of impartiality and of "inflating" the results during the last election for a new assembly to rewrite the Venezuelan constitution (Barboza Gutiérrez, 2014; BBC, 2017; Oppenheimer, 2015).

The second Internet shutdown in Venezuela took place between February 19-22, 2014, over 30 hours, and it occurred in San Cristóbal, the capital city of Táchira, the border state between

Venezuela and Colombia (Kerr, 2014). Since 2014, Venezuela's inflation increased over 50% and foreign currency valuation sites were blocked massively. However, in February 2014, when the highest increased in inflation occurred, protests in the border state of San Cristóbal also increased. Hundreds of blogs and sites, especially the ones containing political news, were censored (these include Twitter and Herdict). In Táchira, the connection to Internet was not available through CANTV (ISP owned by the government) or any other ISP (Diaz, 2014; ONG Derechos Digitales, APC, & Varon Ferraz, 2014). Representatives of the Venezuelan government blamed protesters of the right-wing groups for the problem and denied any responsibility in the Internet shutdown (Frank Bajak & Sequera, 2014).

Former Venezuelan Science and Technology Minister Manuel Fernandez (2014)	When asked about the shutdown of the Internet in the city of Táchira, he stated: "En algunos casos se producen cortes de la fibra por accidentes, en otros por hechos de vandalismo, pero siempre procedemos a empalmarlos para optimizar el servicio. En esta ocasión, tuvimos problemas en la zona norte de Táchira y dentro de San Cristóbal con algunas tanquillas, porque se han presentado muchas quemas en la ciudad" (Noticias24, 2014, para.3) ".. lo que están haciendo esos grupos minoritarios, fascistas, violentos contra la patria es una cosa inaceptable, le están quitando la tranquilidad y la calma a los niños, hombres y mujeres de este país, y una de las expresiones claras de esa agresión son los ataques a CANTV…" (SOSVenezuela2014, 2014, 0:29) Hay que recordar que Cantv le sirve a 22 millones de venezolanos, empresa a través de la cual el Estado ofrece acceso a las telecomunicaciones para todas y todos, sin distingo político" (AVN, 2014, para.5) ".. los incendios van por las taquillas por dónde va la fibra óptica" (SOSVenezuela2014, 2014, 3:37) "163 páginas web del Estado fueron saboteadas en doce días" (SOSVenezuela2014, 2014, 6:48)

	Translation: "In some cases, fiber optic cables may get cut by accident, in some others for vandalism, but we always proceed to splice them to optimize the service. This time we had problems in the northern zone of Táchira and inside the state of San Cristóbal with some sewers because there were a lot of fires in the city" "… those minority groups, fascists, violent, against the motherland is unacceptable, they are taking the tranquility and calm from children, men and women of this country, and one of the clearest expressions of that aggression is the attacks against CANTV …" "We must remember that Cantv serves 22 million of Venezuelans, this is a company through which the government provides access to telecommunications for everyone, without political distinction" "Fire goes through the sewers and the optic fiber cable" "163 web pages of the government were hacked in the last twelve days"
Former President of CONATEL (Venezuelan Regulator) William Castillo (2014)	When asked about the activities of the Venezuelan government over the Internet in Táchira, before the Internet shut down, he stated: "Bloqueamos varios de los enlaces desde donde se atacan sitios públicos. Se mudan a nuevas direcciones. Mantenemos el monitoreo permanente" (El Universal, para.1, 2014) *Translation:* "We blocked several links that attempted to hack public websites. Hackers move to new addresses. We keep monitoring permanent"

Both scenarios in Venezuela are of course very different, and they provide two different insights of what the government tried to achieve when they shut down the Internet. In the first case, the government acknowledged that they did shut down the Internet. They also said it was to protect the government's social network accounts and public agencies sites, both which were used as communications means by the government. In the second case, the government denied any

responsibility in the shutdown and they blamed the political protesters against the administration of Nicolás Maduro.

In both cases, 2013 and 2014, Venezuela was facing massive political protests against the administration of Nicolás Maduro, the questioned current president[29] (El Comercio, 2014; Neuman, 2013). As the literature has suggested (for authoritarian and hybrid regimes), in both episodes, the Venezuelan government was trying to limit the accountability of its actions by preventing political mobilization and public protest (Howard et al., 2011; Michaelsen, 2016). As the facts developed, during the first episode the Venezuelan government blamed a foreign hacker of attacking their communication capabilities, and in the second they blamed protesters of destroying the Internet infrastructure. Despite of the government explanation for the second case, Twitter made public the Venezuelan government censored that social network (Obrien, 2014).

In both cases, audiences are not instrumental to achieve an Internet shutdown. In the first case the government speech points out that an attempt to control the flow of information was the cause to shut down the Internet. Actions follow what the Venezuelan government called a foreign attack, but at the end they were trying to preserve their own communication means. In the second case, the government censored the same platform, Twitter. In both cases, the audience is again the social networks. Social networks are not instrumental to achieve an Internet shutdown, but they are the "carriers" of information that the Venezuelan government wants to control since the times of Hugo Chavez.

[29] On January 23, 2019, Mr. Juan Guaidó, 10th President of the National Assembly of Venezuela, took a public oath to serve as interim President of Venezuela. Guaido's legal claim is based on an interpretation of Article 233 of the Constitution of Venezuela (Herrero, 2019).

Additionally, and not in the same terms, owners of the Internet infrastructure are also the audience. The government-owned-CANTV controls around the 90% of the Internet subscribers in Venezuela, however the remaining 10% have some points of international connection to move the information abroad (Dyn, 2012, 2014b). Within this context, the government wants to control the 10% of Internet users that CANTV does not support. According RESORTE, those users are data managers that are partially responsible for what is posted and happens online. In a sentence, they are responsible for the information posted online and the way the information flows. In the terms of the government representatives, these users certainly may include foreign hackers and destroyers of the Internet infrastructure. The audience they intend to convince, using terms of "fear," is the segment of the Internet they cannot control, the segment that handles information the government dislikes but that cannot control.

4.3.3.2.Referent Object

The referent object is one of the most important elements within the security discourse. From the referent object depends the type of policy governments decide to implement, the audience to address and the content of the speech. As explained before, there can be one or more referent objects. The referent object is deemed worthy of survival and can be assimilated to the national interest, that thing or things that need to be protected to guarantee the national security of a nation-state (McDonald, 2008).

At this point it is necessary to remember that the securitization theory refers to a speech act in which an actor makes a claim that some referent object (s) is existentially threatened. The

securitization theory justifies the use an extraordinary measure to protect the referent object by fighting against the threat (Jutila, 2015).

4.3.3.2.1. Consolidated Democracies

The security discourse for consolidated democracies shows that the most important referent object for consolidated democracies is the critical infrastructure, mostly owned and handled by the private sector. As explained before, the referent object is defined as the thing or things that must be protected to guarantee the national security. In this condition, the referent object is also the national interest, the main element to protect within national security policies because its protection is tied to the survival and stability of the nation-state. In this regard, I identified the critical infrastructure as a common element of all national security policies, independently of being a consolidated or a young democracy. However, the critical infrastructure is not the only referent object. Consolidated democracies are also worried about the control of social network platforms when these endanger what they consider the "public order" that the government is habituated and can handle.

The next paragraphs will provide evidence for these conclusions. Some statements have been previously mentioned to analyze the audience, this time they will be used to identify the referent object.

The U.S. will be our first case. As illustrated before, during the 111th Congress, bills S.773 and S.3480 were in the middle of the debate because they would have authorized emergency measures by the president if the U.S. critical infrastructure was threatened by a cyberattack. Similar provision was contained in S. 413 during the 112th Congress (E. A. Fischer, 2014). These are some

of the statements of sponsors and supporters of the bills on the subject. All of them referred to the protection of the critical infrastructure as the referent object, that thing that will preserve the security and survival of a nation-state.

Former Senator John Rockefeller (U.S.) (2009)	*About S.773* "We must protect our critical infrastructure at all costs—from our water to our electricity, to banking, traffic lights and electronic health records—the list goes on … if we fail to take swift action, we, regrettably, risk a cyber-Katrina." (Aquino, 2009, para.6) "I know the threats we face, … Our enemies are real. They are sophisticated, they are determined and they will not rest." (McCullagh, 2009, para.6)
Former Senator Joseph Lieberman, Senator Collins and Senator Carper (U.S.) 2011	*About S.3480* "The federal government must ensure that SCADA* systems controlling our most critical infrastructure are not just minimally protected, but that they all maintain a high level of security consistent with the risk that a disruption could cause catastrophic damage. To achieve the security we need, S. 3480 would establish a collaborative, cooperative partnership between our most critical infrastructure" (U.S. Senate, 2010, p.9) *Supervisory control and data acquisition
Former Senator Joseph Lieberman, (U.S.) 2010	*About S.3480* "In the event of a catastrophic cyber-attack that could seriously jeopardize public safety, our economy, or our national security, the bill provides the President with the authority to initiate emergency measures to protect our most critical infrastructure" (Lieberman, 2010b, p.3)
Republican staff director and counsel for the Senate Homeland Security and Governmental Affairs Committee Brandon Milhorn (U.S.)	*About S.413* "The point of the proposal is to assert governmental control only over those "crucial components that form our nation's critical infrastructure"" (McCullagh, 2011b, para.4)

2011

Former Senator Joseph Lieberman, (U.S.) 2010	*About S.413* "For all of its 'user-friendly' allure, the Internet can also be a dangerous place with electronic pipelines that run directly into everything from our personal bank accounts to key infrastructure to government and industrial secrets" (McCullagh, 2011, para.9)

In a similar way, the White House proposal also points out to the critical infrastructure as the referent object:

Statement for the Record of Philip Reitinger, Deputy Under Secretary National Protection and Programs Directorate, DHS and others (U.S.) 2011	*About the White House Proposal: Cybersecurity Regulatory Framework for Covered Critical Infrastructure:* "Our critical infrastructure – such as the electricity grid, financial sector, and transportation networks that sustain our way of life – have suffered repeated cyber intrusions, and cyber-crime has increased dramatically over the last decade." (Phillip Reitinger et al., 2011, para.4) "The proposed legislation is focused on improving cybersecurity for the American people, our Nation's critical infrastructure, and the Federal Government's own networks and computers" (Phillip Reitinger et al., 2011, para.9)

I must also add that, since 2009, the White House has addressed the importance of the cyberspace and the digital technology within the U.S. national security policies. In this regard, the White House took a clear stand to protect what they called the "nation's cyber infrastructure":

President Barack Obama (U.S.) 2009	*Remarks of President Barack Obama on Securing the Nation's Cyber Infrastructure, Washington DC, May 29, 2009:* "… From now on, our digital infrastructure – the networks and computers we depend on every day- will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage" (Springer, 2017, p.325)

Although there are no explicit calls of the U.S. to regulate the Internet, this statement may be included as a cybernationalist call.

At this point it's important to make a parenthesis specifically about the U.S. case. As it can be seen, all previous discourses were from U.S. government representatives were mostly related to the protection of the critical infrastructure. However, in 2015 the discourse changed dramatically. Back on December 7, 2015, the Presidential Republican Candidate Donald Trump addressed a crowd of supporters in South Carolina while talking about banning Muslims citizens of entering U.S. territory. During that appearance, Mr. Trump proposed restrictions to Internet access for some individuals as part of a counterterror plan to fight against the Islamic State in Iraq and Syria (ISIS), also known as ISIL or Daesh, online (David, 2016; Goldman, 2015; Hautala, 2015):

> "We are losing a lot of people to the Internet. We have to do something. We have to go see Bill Gates and a lot of different people that really understand what's happening. We have to talk to them about, maybe in certain areas, closing that Internet up in some way ... Somebody will say, 'Oh, freedom of speech, freedom of speech.' These are foolish people, we have a lot of foolish people, we have a lot of foolish people because they are recruiting by thousands." (Hernando, 0:15, 2015)

Two years after, on September 15, 2017, after an attack over the London underground by a Crude Bomb, the already 45th President of the U.S. made a statement using his Twitter account:

> "Loser terrorists must be dealt with in a much tougher manner. The internet is their main recruitment tool which we must cut off & use better!" (Trump, 2017).

Like in his previous statement, Mr. Trump reinforces his idea of considering the Internet a tool for terrorists as a reason for what he believes to "cut off & use better".

Most likely Mr. Trump was not thinking to shut down the Internet entirely, but to look for ways to deny it to ISIS and its allies (Markoff, 2015), however, what Mr. Trump believed Bill

Gates could do is not clear (LaCapria, 2015). In any case, his speech differs entirely from the previous ones the U.S. government offered. Mr. Trump did not refer at all to the protection of the critical infrastructure, but to stopping the proliferation of a radicalized speech within the Internet, in concrete, the one from ISIS. Therefore, Mr. Trump's statement is not related to the critical infrastructure or the possibility of the U.S. suffering a massive cyberattack; this is a case of speech and public order.

In any case, going back to the critical infrastructure, this is a vital element also for other democratic regimes. As mentioned before, a representative of the Department for Culture, Media and Sport from the U.K., stated that they would consider an Internet shutdown only if the nation-state faces a "… very serious threat for these powers to be used, something like a major cyber-attack" (Hardings, 2011a, para.13). In this regard, and according the U.K. government, since 2011 until today, the number of cyberattacks that increased the most and are of the most concern for the U.K. government, are the ones related to the critical infrastructure. Having the same view as the U.S., the critical infrastructure is also vital for the survival of the U.K. and in that way is treated by the most recent cyber security policy of 2016 (POST, 2011, 2017).

Additionally, about the U.K., I also mentioned previously how that government considered briefly shutting down the Internet during an event of national unrest, such as the riots of 2011. Considering that it is possible to have one or more referent objects, it is important to point out that in this case, the referent object was the internal public order the government is used to and is capable of handle. Although democratic regimes are consistently and constantly worried about the protection of the critical infrastructure, for the specific case of the U.K., the critical infrastructure is not the only referent object. The existence of one or more referent objects is possible according the terms of the securitization theory. In this regard, the U.K. security discourse includes two

referent objects: the vital critical infrastructure (as I detailed before) and the internal public order. Moreover, as it was also mentioned previously, the debate surrounding an Internet shutdown in the U.K. stopped because of possible comparisons with practices in authoritarian regimes, particularly China and Egypt.

Also, as mentioned previously, after these events, former British Prime Minister Cameron tried to create a legal framework to control the social network platforms (Facebook and Twitter) and in this way, to control the flow of information (Halliday, 2011b). Mr. Cameron referred to the flow of information during these events, as flow of information used for ill because it helped to coordinate activities that affected the order in the city in the way the government is used to handle and coexist (Cameron, 2011a).

As for the last case, the Australian one, it was already mentioned the importance of the critical infrastructure. Since 2008, former Communications Minister Steven Conroy, warned about the dangerous of having the Internet connected to the Australian critical infrastructure: (Senator Stephen Conroy, 2008):

Author: Former Minister for Broadband, Communications and the Digital Economy Stephen M. Conroy (Australia)	"The internet and wireless links can operate and control power, water, transport and broadcasting. … Because of the access it can provide, it also poses a significant risk to the protection of critical infrastructure and government information systems" (Senator Stephen Conroy, 2008, p.9)

Following his approach, in 2009, the Australian government set as a strategic priority the protection of the critical infrastructure (Australian Government, 2009a). Same approach would be consolidated in the Australian cyber security strategy of 2016 (HM Government, 2016).

4.3.3.2.2. Hybrid Regimes

Hybrid regimes fear a constant intrusion by other nation-states in their own internal affairs and, at the same time, they deny any intention from isolating themselves from the rest of the international traffic. However, as I will depict in this document, they also carry on activities that show the opposite, this is that they do intend to implement policies to keep their Internet infrastructure under government control. At the same time, if the Internet infrastructure is damaged, hybrid regimes tend to blame a third party for that (Bernard, 2015; Costello, 2017; Anastasia Golitsyn, Sergina, & Kozlov, 2016; RT, 2014c; SOSVenezuela2014, 2014; UN, 2014a; Venprensa, 2013). In these cases, there are different possibilities about what the referent object is; as I will explain, the two cases under study (Russian and Venezuela) reflect different national interests: 1) Venezuela is concerned with the attack over the social network platforms the ruling party uses to communicate and some public pages the government uses with the same purpose, 2) Both, Venezuela and Russia, are concerned with the flow of information. In this regard, the next paragraphs will provide detail of how these elements became the referent object of these hybrid regimes that prompted them to shut down the Internet.

In 2010, when former Venezuelan President Hugo Chavez was still alive, he called for a regulation of the Internet that according to him, reports false information. As he stated: “The Internet cannot be something open where anything is said and done. Every country has to apply its own rules and norms” (Chinea & Daniel, 2010, para.2). In March of that year, the hashtag #freevenezuela was largely used after several TV stations were shut down by the government (seven of every ten people became critical of the president), Chavez declared that “the Internet is a battle trench because it is bringing a current of conspiracy” (Hopkins, 2015, para.7).

Facing Chavez fears, the Venezuelan government included the Internet in the law on social responsibility on radio and television, RESORTE, as referred in previous chapters. However, despite of this measure, in 2010 Hugo Chavez himself joined to Twitter. He would use this account to send orders to his ministers and to respond directly to Venezuelan citizens' tweets and therefore, he used Twitter as its own communication platform. He also would use to anger other nation-states with his comments. When Hugo Chavez was no longer visible, his Twitter account was still active (Burke, 2017).

As I established in my previous analysis, in 2013 during the presidential elections, it would be the protection of these communication platforms and the so call protection of public pages, what prompted the shutdown of the Internet. When presenting the Venezuelan case, I reported that, back in 2013, the Venezuelan government claimed that a foreign hacker hacked the Twitter accounts of the current president, Nicolás Maduro, and the ruling party.

At the beginning of 2014, during the protests in Táchira, the government censored social networking services and removed foreign channels from the Venezuelan TV cable. At the same time, the government claimed that TV stations could be in violation of the law on social responsibility on radio and television, RESORTE, a law that forbids any action against what the government considers to be the public order. ISPs that conduct business in Táchira shut down their services and the explanation of the government came from two different individuals: 1) CONATEL's former director, William Castillo, claimed that the government was trying to protect public sites, that is why they censored the Internet. Exactly what he meant by "public sites" was never clarified and 2) the former Venezuelan Science and Technology Minister, Manuel Fernandez, blamed protesters for the entire shut down the Internet, accusing them of damaging the Internet infrastructure and denied any responsibility of the government.

Former President of CONATEL (Venezuelan Regulator) William Castillo (2014)	"Bloqueamos varios de los enlaces desde donde se atacan sitios públicos. Se mudan a nuevas direcciones. Mantenemos el monitoreo permanente" (noticias24, para.2, 2014) "Los ataques cibernéticos contra Venezuela continúan desde diversos lugares del mundo" (noticias24, para.3, 2014) *Translation:* "We blocked several links from where public sites are hacked. Hackers move to new addresses. We keep monitoring permanent" "Cyber attacks against Venezuela continue from different places around the world"
Former Venezuelan Science and Technology Minister Manuel Fernandez (2014)	"En algunos casos se producen cortes de la fibra por accidentes, en otros por hechos de vandalismo, pero siempre procedemos a empalmarlos para optimizar el servicio. En esta ocasión, tuvimos problemas en la zona norte de Táchira y dentro de San Cristóbal con algunas taquillas, porque se han presentado muchas quemas en la ciudad" (Noticias24, 2014, para.3) ".. los incendios van por las taquillas por donde va la fibra óptica" (SOSVenezuela2014, 2014, 3:37) "163 páginas web del Estado fueron saboteadas en doce días" (SOSVenezuela2014, 2014, 6:48) *Translation:* "In some cases, fiber optic cables may get cut by accident, in some others for vandalism, but we always proceed to splice them to optimize the service. This time we had problems in the northern zone of Táchira and inside the state of San Cristóbal with some sewers because there were a lot of fires in the city" "Fire goes through the sewers and the optic fiber cable" "163 webpages of the government were hacked in the last twelve days"

Although the director of CONATEL did not talk about an Internet shutdown but a censoring policy, the explanation about protecting public sites is the same that former vice-president Jorge Arreaza gave during the Internet shutdown of 2013 (Bracci Roa, 2013).

The other case under analysis, Russia, shows fear of the U.S. and its allies. Their initial concerns started after the annexation of Crimea and got worst after the Snowden revelations (Lipman, 2014; Madory, 2014). As depicted before, Russian authorities became very concerned about their data, from the government itself and its citizens. This is the reason for constant claims and legislative actions of the Russian authorities to force foreign companies like Google to keep any Russian data in servers located within Russian territory.

Nevertheless, it is not only the data itself what Russians are worried about. They are also worried about its management, or the flow of data, who controls and circulates it. According to the Information security doctrine of 2016, Russia want a nation system to manage RuNet because according to the Russian mindset the Internet is a dominant U.S. product and therefore, the free flow of information is a threat to the Russian cultural integrity and independence (Nikkarila & Ristolainen, 2017).

However, this fear of the Russian government is not new. In the mid-sixties, the former Soviet Union, criminalized "the dissemination of intentionally false insinuations defiling the Soviet state and the social order" (Lipman, 2014, para.1). Of course, the dissemination of information back in those days was limited to the technology of the time: radio, typewriters, copy machines among others. All these forms of communication were, with a high level of success, intercepted or controlled by the Russian government.

In today's time, the situation changed radically with the Internet, a tool where attribution is not easy to determine and where free public exchange is still possible at some extent. It is this

free exchange and free flow of information what Vladimir Putin is afraid of (Lipman, 2014). This fear is the reason why the Russian president called the Internet a "CIA project" (MacAskill, 2014).

As I also analyzed previously, Russian authorities claimed that the "unpredictable west" can "disconnect" RuNet from the global Internet and compromise the integrity of the Internet itself and the personal data of Russian citizens (Belousov, 2014). Following this tendency of Russian cyber nationalism, the new laws enacted by the Russian government, required all online companies to store Internet users' personal data within Russian territory and targeted cyber activism, bloggers, market players and social networks originating from abroad, such like Facebook and Twitter (Hille, 2015; Zavyalova, 2014).

This fear of free flow of information can be appreciated in two cases within the Russian context:

1. Yandex, a Russian search engine, is responsible for more traffic in Russia than Google, but Vladimir Putin accused the company of not being nationalist enough. Putin accused Yandex for having a number of Europeans and U.S. citizens in its governing bodies and because "they had to agree with that" without major objection (Lipman, 2014, para.7)
2. After the annexation of Crimea, the Russians quickly joined the peninsula to RuNet. Russian Prime Minister Dmitry Medvedev stated that "it is necessary to ensure that [state-owned Russian telecommunications company] Rostelecom and its subsidiaries come to Crimea as quickly as possible" because "sensitive information and documents ... are [being] relayed by foreign telecommunications companies" (D'Orazio, 2014, para.2)

As a logical parallel to this Russian nationalistic policy, Russia's Oversight Communication Agency (Roskomnadzor) warned Google, Facebook, and Twitter that they must be registered as "organizers of information distribution" in compliance with the law (Koshkin, 2014). At the end of 2016, Roskomnadzor proposed to block LinkedIn in Russia because this social network failed to transfer Russian user data to servers located within Russian territory, in clear violation of the national law. This action of the regulator makes effective a court ruling from a Moscow City Court. At the time of the LinkedIn blocking, Facebook and Twitter still kept their data housed out of Russian territory, while Apple and Google had complied with the Russian law (Lunden, 2016; Reuters, 2017a; Tsvetkova & Osborn, 2016).

The cases previously mentioned show how important is for the Russian government to control the data about itself and its citizens. I concluded before, as stated by Russian authorities, that an attack that can trigger an Internet shut down is an attack from a foreign power (most likely the U.S.) that: 1) would make the Russian government to lose control over its own data and its citizens' and that 2) would make the Russian government to lose control over the Internet infrastructure. These two scenarios are only possible because of the actions of private companies based in the U.S. that handle Russian data.

The Russian case, differently from the Venezuelan one, presents one more referent object. Again, I must bring into account that the securitization theory of the Copenhagen School allows for one or more referent objects. In the same line of the democratic regimes, Russia is also interested in the protection of the critical infrastructure of that nation-state. This became a public claim in 2016, when the Obama administration blamed the Russians for its interference during the 2016 presidential election (Nakashima, 2016; Adam Taylor, 2016). Back then, German Klimenko,

Vladimir Putin's Internet adviser suggested that Russia could disconnect itself from the global Internet during a crisis:

> "In the law we are talking about the protection of critical infrastructure, which should be located in the territory of Russia … For example, hackers can penetrate the structure of commercial banks and steal money. This is bad, but if they enter into the system of the Central Bank, we would be in big trouble." (Adam Taylor, 2016, para.4; Astakhov, 2016, para.2)

In the same year 2016, in May, a representative of *Minkomsvyaz*, the Russian Ministry of Communications and Mass Media, announced plans to protect the Russian critical infrastructure:

> "… by 2020, 99% of Russian internet traffic should be transmitted within the country and that it is going to create a 'back-up-copy' of 99% of the 'critical infrastructure' within Russia." (Translated by Nikkarila & Ristolainen, 2017, p.2)

Klimenko also pointed out that western powers block the access of Google and Microsoft services into Crimea after its annexation as a product of the U.S. sanctions. He advocated for an independent Russian Internet. According Klimenko, Russia should have the possibility of shutting down RuNet and keep it independent of the global Internet:

> "There is a high probability of 'tectonic shifts' in our relations with the West, … Therefore, our task is to adjust the Russian segment of the Internet to protect themselves from such scenarios … critical infrastructure should be on Russian territory, "so no one could turn it off" (Adam Taylor, 2016, para.4; Astakhov, 2016, para.2)

At this point it is important to go back to the clarifications I mentioned in the chapter three, when describing the Russian case. The statements of the Russian securitizing agents indicate that the government has two different approaches when considering an Internet shutdown. On one hand, there is a concern over the foreign enemy (the "West") imposing its will and shutting down the Russian Internet, and on the other hand, it is the perspective of an action of the Russian government itself shutting down RuNet under circumstances of national security (Vargas-Leon,

2018). The two perspectives include an Internet shutdown as the result of a government action and an Internet shutdown provoked by foreign enemies in the form of a cyberattack.

As it can be inferred as a conclusion is that, just like in the U.K. case, there is more than one referent object for hybrid regimes: the data itself and the critical infrastructure. Hybrid regimes tend to blame third parties for their decisions to act over the Internet infrastructure. This is the case for Russia blaming to the U.S. government and the "West," or Venezuela blaming foreign hackers or internal protesters.

Tables 04 and 05 summarize the elements of the securitization theory in democratic and hybrid regimes as they have been explained in this chapter.

Table 04.- Elements of the Securitization Theory in Democratic Regimes

Nation-State / Units of Discourse Securitization Theory Copenhagen School	Australia	U.K.	U.S.A.
Securitizing Agent	1. Stephen Conroy Former Minister for Broadband, Communications and Digital Economy	1. David Cameron Former Prime Minister 2. Sir Nick Harvey Former Minister of State for the Armed Forces 3. Representatives of the Department for Culture, Media and Sport	1. Former Senator John ("Jay") Rockefeller 2. Former Senator Joseph ("Joe") Lieberman 3. Senator Susan Collins 4. Philip Reitinger, Former Deputy Under Secretary National Protection and Programs Directorate, DHS

Speech Act 1. **Grammar of Security (protection of the Referent Object)** 2. **Threat Subject** 3. **Extraordinary Measure**	1. Internet: threat to critical infrastructure, stability of the government information system 2. The critical infrastructure is vital for the survival and security of the nation-state 3. Distrust towards management policies of the ISPs 4. Internet must be regulated by national governments. Any strong policy must be decided by the government 5. An Internet Shutdown is not considered explicitly, but the terminology "any measure" may include it 6. The Internet must be regulated	1. Internet: threat to critical infrastructure, stability of the government information system 2. The critical infrastructure is vital for the survival and security of the nation-state 3. Internet must be regulated by national governments. Any strong policy must be decided by the government 4. An Internet Shutdown is explicitly considered	1. Internet: threat to critical infrastructure, stability of the government information system 2. The critical infrastructure is vital for the survival and security of the nation-state 3. An Internet Shutdown is explicitly considered 4. Cybernationalism: the digital infrastructure is a strategic national asset
Audience **The one that needs to be convinced to achieve the protection of the referent object**	1. The private sector that owns and handles the critical infrastructure	1. The private sector that owns and handles the critical infrastructure 2. Massive Communication Means: f/e social network platforms	1. The private sector that owns and handles the critical infrastructure
Object to Protect	Critical Infrastructure	1. Critical Infrastructure 2. Internal Public Order: keep social control in the way the government is used to handle it	Critical Infrastructure

Table 05.- Elements of the Securitization Theory in Hybrid Regimes

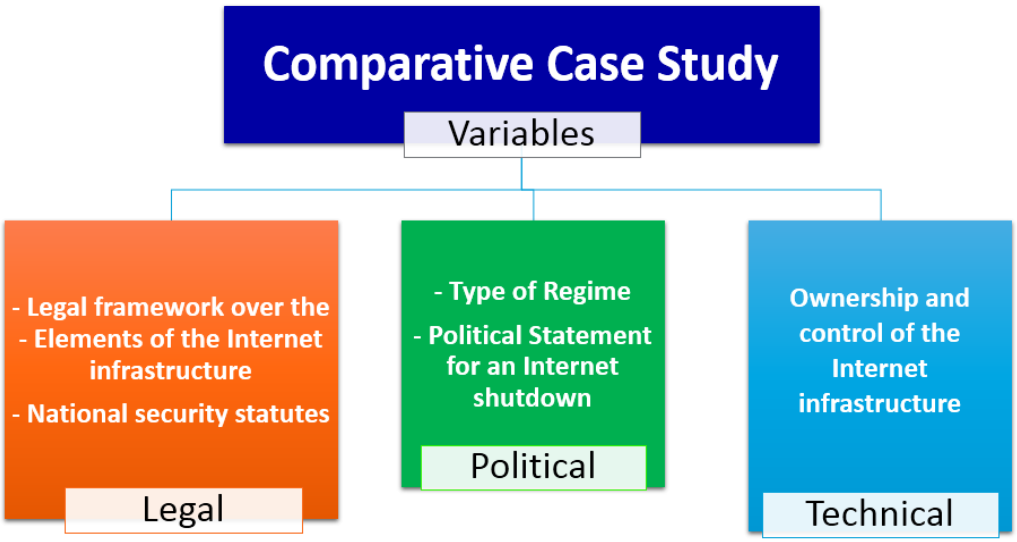
Nation-State / Units of Discourse Securitization Theory Copenhagen School	Venezuela	Russia
Securitizing Agent	1. Hugo Chavez Former Venezuela President (Deceased) 2. Jorge Arreaza Former Venezuelan Vice President and Minister of Science and Technology 3. William Castillo Former President of CONATEL (the Venezuela regulator) 4. Manuel Fernandez Former Venezuelan Minister of Science and Technology	1. Vladimir Putin Current President of the Russian Federation 2. Igor Shchegolev Former Communications Minister and Aide to President Vladimir Putin 3. Dmitry Peskov Presidential Press Secretary of the Russian Federation 4. Vladimir Medinsky Minister of Culture of the Russian Federation 5. Dmitry Rogozin Deputy Prime Minister of the Russian Federation 6. Leonid Levin Chairman of the State Duma Committee on Information Policy, Information Technology and Communications 7. Yevgeny Fyodorov Deputy of the State Duma of the Federal Assembly of Russia 8. Ilya Kostunov, Ruslan Gattarov, Lyudmila Bokova The three of them, Members of the State Duma

Speech Act 1. **Grammar of Security (protection of the Referent Object)** 2. **Threat Subject** 3. **Extraordinary Measure**	1. The Internet cannot be free 2. Cybernationalim: Every nation-state should be independent when legislating about the Internet 3. Enemies are foreign hackers and protesters against the regime: they are enemies of the revolution 4. Shutting down the Internet was neccesary to protect official "public pages" and the communication platforms of the rulling party, Twitter in particular 5. They deny any intention of isolating from the international Internet traffic	1. Cybernationalim: Every nation-state should be independent when legislating about the Internet 2. Enemies of Russia are the U.S. and its allies, the "impredictable west": they are conducting a "blitzkrieg" against Russia 3. The U.S. and its allies could disconnect RuNet from the rest of the international Internet traffic 4. The Russian government denied any intention of isolating RuNet from the international Internet traffic. However, the Russian government may, on its part, be forced to shut down RuNet in order to protect the Russian national security and for the protection of the critical infrastructure 5. In order to achive its war against Russia, the U.S. uses private companies such as Google, Facebook or Twitter, because they can storage data about Russian citizens and the Russian government in servers located within U.S. territory 6. Data of Russian citizens may be compromised 7. The Internet was crated to weaken Russian stability, therefore Russia must have its own Internet
Audience **The one that needs to be convinced to achieve the protection of the referent object**	1. ISPs as data managers, they are partially responsible for what is posted online 2. Social media platforms, Twitter in particular	1. Private companies that handle Russian citizens' data and the government data, f/e Google, Facebook, Twitter, LinkedIn
Object to Protect	Communication platforms of the ruling party	1. Data from Russian citizens and specially the Russian government 2. Critical Infrastructure

4.4. Answer RQ3: What are the political, legal and Technical factors that enable democratic and hybrid governments to shut down the Internet or to consider doing so?

To analyze RQ3 this dissertation uses, as explained before, a comparative case study. In each case, and to perform a comparison, this dissertation analyzed the variables contained in the figure 19 (see below).

Figure 19.- Variables Comparative Case Study



Before providing an answer to RQ3, it is necessary to present an overview of the variables of each case study (Please see table 08). The subsequent paragraphs will detail and explain the different factors that prompt a democratic or hybrid government to shut down the Internet or to consider doing it, and therefore, they will answer RQ3.

The analysis includes regimes that shut down the Internet or considered doing so: U.S., U.K., Australia, Venezuela and Russia. For purposes of comparison there are similar political

regimes (hybrids and democracies) that did not consider and did not shut down the Internet: Brazil, Mexico and Turkey. The last three cases for comparison are highlighted in different colors.

The purpose of this comparison is to analyze similar regimes, similar in the sense of political classification, whether they are democracies or hybrid regimes, to try identifying the real reasons why a government would shut down the Internet. When analyzing each case, there will be references to the information provided in the description of each case study that was presented in previous chapters.

Sub chapters following table 08 (see in the next page) will explain the different political, legal, technical and economic factors that enable a democratic and hybrid regime to shut down the Internet or consider doing so, and in that way, they will answer RQ3

Table 06.- Technical and Legal Elements to Consider in each Case-Study

NATION-STATE	TYPE OF REGIME	INTERNET SHUT DOWN CONSIDERED (C) HAPPENED (H)	LEGISLATION	IXPs (APPROXIMATELY)	ISPs (APPROXIMATELY)	INTERNET PENETRATION RATE (ANNUAL %) 2015
U.K.	Consolidated Democracy	C	Communications Act of 2003 Civil Contingency Act of 2004	24	Four ISP (>70% traffic) 3000 (30% traffic)	92%
U.S.	Consolidated Democracy	C	Telecom Law 1934, 1996, Bills S.773,3480, 773, Protocol SOP 303	178	Four ISP (>70% traffic) 3500-4000 (30% traffic)	74.45%
Australia	Consolidated Democracy	H	Telecommunications Act from 1979 and amendments of 1997 and 2003 Australian Security Intelligence Organization Act 1979 and amendments of 2001	18	One ISP (>90% traffic) + 44 (10% traffic)	84.56%
Mexico	Young Democracy	None	Amendment to the Federal Telecommunications Law Mexican Constitution of 1917 and amendments of 2014	01	16	57.43%
Brazil	Young Democracy	None	"Marco Civil Da Internet" (Civilian Framework)	37	15	59.08%
Russia	Hybrid	C	Russian 'Blitzkrieg laws' over the Internet infrastructure (2012-2016)	25	18	70.10%
Turkey	Hybrid	None	Law No. 5651, Law 6518 (2014)	03	Government-owned-ISP (>90% traffic)+ 9 (10% traffic)	53.74%
Venezuela	Hybrid	H	The Law of Social Responsibility and Quality of the Television in Venezuela (2005, modified 2010)	00	Government-owned-ISP (>90% traffic) + 7 (10% traffic)	61.87%

4.4.1. Political Factors (PF)

The political factors referred to a nation-state political situation within a specific time. These factors address the governments' leadership, decisions and debate that may affect individuals or organizations. Some of these factors may include government policies, government stability and upcoming regulations (PESTLE, 2015a, 2015b). Table 07 details the main political factors this project identified.

Table 07.- Comparison Political Factors that enable Hybrid and Democratic Regimes to Shut Down the Internet or to Consider Doing So

Factor / Nation-State	Internet Shut Down: Considered (C), Happened (H), None (N)	Fear of a Cyber-attack over the CI (Cyber Pearl-Harbor)	Fear of a Foreign cyber attack	Use of Social Platforms or Message Systems (by Internet Users) during Times of National Unrest or Public Protest	Claims of National Sovereignty over the Internet, (a.k.a. Cyber-Nationalism)	Political demands to Increase the Internet Access	Facilitate the existence of self-defense forces and fight against drug dealing
Russia	C	x	x		x		
Venezuela	H		x	x	x		
Turkey	N			x			
U.S.	C	x		x	x		
U.K.	C	x		x	x		
Australia	H	x			x		
Brazil	N	x		x	x		
Mexico	N					x	x

4.4.1.1. Cyberattack over the Critical Infrastructure, a.k.a. Cyber Pearl-Harbor

As mentioned earlier in this dissertation, IT professionals and members of the U.S. government created the term "Cyber Pearl-Harbor" to describe a massive cyber-attack on nation-states' critical infrastructure. Theoretically, the attack is supposed to be so disruptive and powerful

that the only mechanism of protection over the critical infrastructure would be to shut down the Internet (Weinberger, 2013). A similar term also used by politicians or academics is “Cyber Armageddon” or “Cyber 9/11” (Valeriano & Maness, 2015).

The protection of the critical infrastructure, and therefore, the concern about the feasibility of a cyber-attack that can damage it is a constant concern for most nation-states. In this regard, the protection of the critical infrastructure is part of the national security policy of the U.S. and the U.K. and other democratic and non-democratic regimes around the world (CPNI, 2017; Gurdus, 2016; Mandarino Junior & Canongia, 2010; Oppermann, 2014; Stoddart, 2016). Both nation-states, the U.S. and the U.K., have considered shutting down the Internet if the critical infrastructure is threaten (Ghosh, 2011; Lieberman, 2010; Lieberman, 2011a; Rockefeller, 2010; Williams, 2011).

When explaining the U.S. as a case study for this project, I addressed the fact that the main objection against the use of the “Cyber Pearl-Harbor” concept lies in the fact that there is no agreement about its clarity or its limits. (H. Farrell, 2013; Lawson, 2016; Weinberger, 2013). However, governments of the U.S. and the U.K. do seem to agree that, if necessary, either the head of the government (President or Prime Minister) or someone close in authority has the capacity to decide and order an Internet shutdown (Marsden, 2011; Phillip Reitinger et al., 2011). Nevertheless, despite of the common aspects there are also differences between both cases. The U.S. has considered the possibility of shutting the Internet when the critical infrastructure is involved. The U.K. also acknowledges the possibility of the doing the same. However, the U.K. government also has considered shutting the Internet for social control purposes (Cameron, 2011b; Williams, 2011). In a different, but also similar way at the same time, the U.S. government has been accused of considering shutting down the Internet for social control purposes. Accusations

followed the “BART episode,” related to the use of the SOP 303 protocol (Bell, 2011; Elinson, 2011).

The protection of the critical infrastructure is an element of concern also for other democracies, like Brazil. However, the Brazilian government rejected the idea of shutting down the Internet. The protection of the critical infrastructure has high priority within the cyber security policy of that nation-state. However, Brazil considered all sorts of measures to avoid at all cost an Internet shut down. Circumstances that prompt the discussion on the subject were related to the World Soccer cup of 2014 and the Olympic Games in 2016. Before these events, potential measures to keep the Internet working in case of social protests also became part of the Brazilian green book of cyber security (Almeida Advogados, 2015; Carpes, 2012; CEPROMAT, 2014; Oppermann, 2014).

4.4.1.2.Foreign Cyberattack

In case of this political factor, a potential foreign cyberattack, the evidence this project found comes from two hybrid regimes, Russia and Venezuela. Both nation-states fear a foreign cyber-attack, however there are two differences when considering these regimes: 1) they have different visions of what the “foreign attack” would be and 2) Russia considered to shut down the Internet, while Venezuela did it. The next paragraphs will present each case.

After the Snowden revelations of 2013, regarding the U.S. surveillance activities worldwide (Lawfare, 2014), two members of the Russian parliament (MPs), MP Ilya Kostunov and MP Ruslan Gattarov, alongside with members of the executive branch, publicly expressed their concern that RUNET (the Russian Internet) could be disconnected by the U.S. from the

international Internet traffic. The Russian authorities even suggested a counter-measure, the possibility of shutting down the Internet by the Russian government itself in case of what they called a "foreign attack". Specifically, they talked about a foreign attack from the "unpredictable West" (the U.S. for the case) (Belousov, 2014; HTB, 2014; Lokot, 2014; Runkevich & Malai, 2014; Watson, 2013). Further statements from Vladimir Putin would reveal that the Russian Security Council was conducting tests over RUNET to evaluate the impact of a potential foreign attack and how to shut down RUNET if necessary (Anastasis Golitsyn, 2014b, 2014a; Lawfare, 2014).

The discussion about the Internet shut down in Russia took place while the government enacted several new laws and regulations over the Internet infrastructure (Eremenko, 2014a). According to the Russian authorities, the purpose of these laws was to strength the stability and resilience of RUNET. However, the bills were created with different purposes, as it was stated in their own text: 1) Owners and operators of websites were obligated to store all information about the arrival, transmission, delivery, and processing of voice data, written text, images, sounds, or other kinds of action, 2) the Russian government allowed itself legally to review all content posted on the Internet, 3) Internet companies would be forced to locate servers handling Russian Internet traffic and Internet users' data inside Russian territory, 4) the regulator would be allowed to block websites deemed extremist or a threat to public order without a court order, 5) money donations in the Internet were restricted, 6) any individual deemed a disseminator or re-disseminator of "extremist materials" would be imprisoned and 7) anonymous access to Internet in public spaces was forbidden (Duffy, 2015).

All these laws belong to a whole legal framework, which purpose is to control the entire infrastructure of the Internet, and with it, the flow of data and the communication process in and

out of Russian territory. This also means that the U.S. (or any other government for the purpose) surveillance activities should not get any information about the Russian government or the Russian population. As a matter of fact, since 2008 Russia has been insisting in the creation of a domestic Internet that recognizes only Cyrillic characters and is separated from the international Internet traffic (Francis, 2008). In 2014, they would make the same claim again (RIA Novosti, 2014). The Minister of culture even talked about a "Patriotic Internet" that can protect Russian citizens from the U.S. espionage activities (Dolgov, 2015a). In 2016 the enactment of new surveillance laws about encryption would be again an example of the control the Russian government wants to exercise over the Internet infrastructure (Galperin & O'brien, 2016; O'Neill, 2016).

For the Russian government, the Internet is a vital part of its own identity and in this regard, it is related to the consolidation of the Russian government power. In fact, in July 2014, Crimean ISPs began receiving Internet services over the newly constructed submarine cable "Kerch Strait Cable," that connected Crimea with Russia. For international analysts the message was clear: there was no turning back in the process of infrastructure consolidation by Russia in Crimea (Madory, 2014).

From a legal point of view, RUNET also must have its own legal framework, which means a specific law for every government activity within the Internet. These laws were also mentioned before in this document and they are known as the Russian "Blitzkrieg" laws over the Internet infrastructure (Eremenko, 2014a, 2014b).

It is possible to conclude that, for the Russian authorities a foreign attack that can trigger an Internet shut down is an attack from a foreign power (most likely the U.S.) that: 1) would make the Russian government to lose control over its own data and its citizens' and that 2) would make the Russian government to lose control over the Internet infrastructure. In this regard, an Internet

shut down is only acceptable if two conditions are met: 1) if it is done by Russian authorities and 2) if it helps to preserve the control the Russian government has over the Internet infrastructure.

Differently from Russia, the Venezuelan government has a completely different idea of what a foreign attack over the Internet is. The first time the Venezuelan government shut down the Internet was in April 2013, during the Presidential elections. Back then, Jorge Arreaza (then vice-President) claimed that foreign hackers attacked the Twitter accounts of the Venezuelan ruling party, "Partido Socialista Unido" – PSUV (United Socialist Party of Venezuela), the candidate Nicolás Maduro (at the time also interim president) and the webpage of the Consejo Nacional Electoral – CNE (National Electoral Council) (AVN/VTV, 2013).

The CNE is the government agency in charge of counting electoral votes and by constitutional mandate it should be independent from any other government institution. However, the CNE impartiality and neutrality was questioned during the 2013 elections and is constantly used as a communication platform by the government (Barboza Gutiérrez, 2012, 2014; Nuñez & Ochoa, 2013). According to Arreaza, in order to protect the CNE webpage and the social platforms of the ruling party and its candidate, the Venezuelan government decided to stop the Internet service. This process took around four minutes in Caracas (the capital city) and 20 in the rest of the Venezuelan territory. This Internet shut down was possible because the government owns CANTV, the ISP that handles over 90% of the Internet subscribers in Venezuela (Diaz Hernandez, 2013; Venprensa, 2013).

Political rivals accused Arreaza and the ruling party of taking these actions to manipulate the electoral data. Arreaza rejected the accusations stating that there was no problem with the Internet and that they were just trying to protect the sites previously mentioned from foreign attacks. As explained before, this was the first time (out of three) that the Internet has been shut

down in Venezuela. In this case, the foreign attack has a different connotation from the Russian one. The Venezuelan government was trying to protect the communication platforms of the ruling party, Twitter accounts and an official webpage. Attackers were supposed to be foreign ones by claim of the Venezuelan authorities themselves, although this was never clarified. Venezuelan has lived many episodes of censorship in the past and they continue, but this was the first time the Internet was shut down (OpenNet, 2013; Reuters, 2017b).

In this case the Internet shut down was not related to the flow of data or information, but to the communications capabilities of the ruling party in times when its "stability" in power was not clear. At this point it is necessary to remember that one of the reasons why Venezuela is considered a hybrid regime is because the same party has been ruling since 1999 (EIU, 2017).

4.4.1.3. Use (By Internet Users) of Social Platform or Message Systems During Times of National Unrest or Public Protest

The idea of shutting down the Internet to interrupt the communication process within social platforms has been used as a reason to shut down the entire Internet, or to consider doing it, in democratic and hybrid regimes. When this occurred, nation-states under analysis were going through a time of national unrest. For the U.K., a consolidated democracy, this was the case during the London riots of 2011 (Casilli & Tubaro, 2011; Ionescu, 2011) and for Venezuela, this occurred in 2014 during the protests against the government of Nicolás Maduro (Frank Bajak, 2014). Each case will be described in the next paragraphs.

As mentioned before, back in 2011, the U.K. Prime Minister Cameron blamed the Black Berry message system, Facebook and Twitter for allowing rioters to organize themselves and

create chaos and disorder in London. Moreover, and not well publicly known, Mr. Cameron suggested shutting down the Internet completely because they could not control the communication within the social networks (Ghosh, 2011; Nosowitz, 2011). The U.K. government decided not shutting down the Internet because he was warned of possible comparisons with the Internet shut down in Egypt and similarities with Chinese censorship policies (MacKinnon, 2012; Williams, 2011). Possible comparisons with dictatorial regimes at the end were important for the U.K. government.

The U.S. also presents a case of trying to control, not social networks, but a message system. This case occurred during the BART episode. As this document explained before, in 2011, all cellular service inside the Bay Area Rapid Transit (BART) got disrupted in San Francisco transit stations for three hours during a mass public protest. In July 2012, the DHS accepted some responsibility in the episode and referred to the SOP 303 emergency protocol (Brownlee, 2015; DeSoto, 2015). Although this is just one episode, it reveals the technical means and capabilities the U.S. government has, to control (at some extent) the Internet. Nevertheless, despite the situation, I don't consider the U.S. as a case of an Internet shutdown for two reasons: (1) it is not known the real capacity of SOP 303 to affect the Internet (in terms of devices -computers, phones, territorial extension or even the content of the protocol) and (2) since only the BART facility was affected, any Internet user or protester who wanted to access the Internet only had to walk out of the building.

The Venezuelan case is different. This situation started back in 2014 in the middle of public protests against Nicolás Maduro. Local media was under censorship and the foreign press was being harassed; in this scenario, the Venezuelan population only had the Internet as a source of news. However, the government started a campaign of repression that started censoring social

networks platforms, specially twitter, and ended up with an Internet shut down. These actions concentrated in San Cristóbal, the capital city of the state of Táchira, by the Colombian border. In San Cristóbal protests against the government were stronger and longer than in the rest of the Venezuelan territory (Frank Bajak, 2014; Chao, 2014).

William Castillo, the director of the Comisión Nacional de Telecomunicaciones – CONATEL (National Commission of Telecommunications) claimed that social networks were invaded by cyber-criminals who attack accounts and manipulate information. At the same time, the Minister of Information, Delcy Rodríguez, claimed that social networks, specially Twitter, are used by perpetrators of violence to create anguish in the population (Frak Bajak, 2014; noticias24, 2014). When the Venezuelan government realized they could not control the flow of information in the social networks, they shut down the Internet for three days in San Cristóbal (Mora, 2014).

Despite of the actions of the Venezuelan government, there is an important point to make for this case in terms of feasibility and success of an Internet shutdown. San Cristóbal is next to the Colombian border; Colombia is one of the nation-states with better connectivity in South America since 2002 (WB, 2017). People only had to cross the border, walking every day, to have Internet access.

In the same year of the Venezuelan protests in Táchira, the Russian government also made a political move. In 2014 the Russian government enacted the so call ‘Bloggers Law’. This new law was enacted in the middle of the discussion about Internet security during national emergency situations. As a matter of fact, a mass protest and the use of social networks was included in the political debate as a specific example of this type of situation.

The new law established that that any site with more than 3,000 visitors per day will be considered a media outlet and therefore, will be responsible for the accuracy of the information

published. The law also implements scanning software that allows the Russian government to review all content posted on the Internet, regardless of daily page hits or classification. In this scenario, bloggers can no longer remain anonymous online. Additionally, any organization that provide platforms for their work and communications, like search engines, social networks and similar forums are required to maintain computer records on Russian soil of everything posted during the last six months (MacFarquhar, 2014).

As the law was passed, there was a common believe among experts and civil activists that the real targets were not just any social platform, but those that originate abroad, like Facebook and Twitter. This believe also is consistent with the new Russian law that requires foreign companies to store data within the Russian borders (MacFarquhar, 2014; Zavyalova, 2014).

Finally, a singular case also comes into place, the control over social networks by the Turkish government. Use of social networks in Turkey has been growing, however this nation-state never considered and never shut down the Internet. Since 2007, the Turkish government (under the ruling of the same party, AK) has blocked social media because of what the government considers offensive content to Turkey or to Turks. The first of these episodes occurred in 2007, when social media presented some videos insulting Ataturk (the founder of Turkey) were posted in YouTube. The platform was blocked until videos were removed. In 2010, because of an incident presented in a video related to Deniz Baykal, leader of the opposition, YouTube was also blocked. In 2013**,** Turkish people protested again against the government in what is known as the "Gezi park protests," related to the re-urbanization plan for Istanbul. These protests made clear the differences between the traditional media in Turkey and the potential created by social networks (Dogramaci & Radcliffe, 2015).

During social protests in 2014, before the presidential elections, YouTube and Twitter were the target of the Turkish government control. This last situation was especially difficult because this time the Turkish government poisoned the DNS in order to control the IP addresses of Twitter, and the public address of Google (Sifir, 2014). Nevertheless, again in 2015 the Turkish government blocked Facebook, Twitter, and YouTube because these platforms circulated pictures of a prosecutor taken hostage and killed by militants. A year later, by November 2016, WhatsApp messaging, Twitter, Facebook and YouTube were all completely blocked again. This episode followed the detainment of 11 Members of Parliament from the pro-Kurdish People's Democratic Party (HDP) (Mesoznik, 2016). As these episodes show, controlling the social networks in times of turmoil is the "modus operandi" of the Turkish government. Shutting down the entire Internet is not part of the Turkish action or security discourse.

4.4.1.4. Claims of National Sovereignty Over the Internet, a.k.a. Cybernationalism

Constant claims of national sovereignty over the Internet are common characteristics of hybrid and democratic regimes. As it will be explained in the following paragraphs, for consolidated democracies such as the U.S. and the U.K., claims of sovereignty over the Internet infrastructure are part of their national security policy. For hybrid regimes, like Russia, claims of sovereignty over the Internet started between 2003 and 2005 during the World Summit on the Information Society (WSIS). These claims came back into their politics after the Snowden revelations back in 2013 and again in WSIS+10 in 2015 (WSIS, 2015).

As referred in previous chapters, on May 29, 2009, the U.S. Executive branch declared the digital infrastructure (including the Internet infrastructure) as a "strategic national asset" to be

protected by the U.S. government and private companies because digital technologies are vital for the survival and prosperity of the U.S. as a nation state. President Obama's speech declared (White House, 2009):

> "From now on, our digital infrastructure – the networks and computers we depend on every day – will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority"

Following the White House executive order, on June 6, 2010, Senator JoeLieberman (D) introduced bill S.3480, titled "Protecting Cyberspace as a National Asset Act of 2010". Senator Lieberman remarked that the Internet is constantly under attack; therefore, the purpose of bill S.3480 was to secure the most "critical cyber-networks" in order to preserve the critical infrastructure that is connected through the Internet networks and that is vital for the survival of the U.S. as a nation-state (White House, 2009).

Two years after declaring the digital technology a national asset, on May 12th, 2011, the Obama Administration prepared a set of recommendations for a new cyber-security legislation including a regulatory framework for covered critical infrastructure (Thompson, 2012; U.S. Senate et al., 2010).

On May 23rd, 2011, a hearing was conducted within the Committee on Homeland Security and Governmental Affairs of the U.S. Senate to assess the White House proposal (Schmidt, 2011). In reference to the possibility of shutting down the Internet, (US Senate, 2011) (at the time, the deputy undersecretary for the National Protection and Programs Directorate, from DHS), referred to the attributions for the president established in the Telecommunications Act of 1934. Mr. Reitinger stated that, because national security situations are "context-driven," any final response about how to act requires further discussion and debate among all the stakeholders involved (Philip Reitinger et al., 2011). Reitinger also acknowledged that although the Telecommunications Act

was not designed for the current cyber-security environment, the president will "use the authority that it brings to bear in the right way" (US Senate, 2011, para.40).

Claims of defense of national sovereignty are also available in the U.K. policy debate, but with reference to the economic well-being of the U.K. Back in 2011, the same year of the riots in London, Sir Nick Harvey (the Minister for the Armed Forces from the U.K.) recognized the cyberspace as a new global domain and the Internet infrastructure, as the main element of the cyberspace. For Sir Harvey, the economic well-being of the U.K. is aligned with the protection of the Internet infrastructure, however, the Internet itself has created connections that do not recognize territorial borders. This is not acceptable for U.K. authorities; for them, the well-being of the U.K. only can be achieved if there is a balance within the Internet between personal freedom, national sovereignty and international stability (US Senate, 2011). The words of the minister are a call for the inclusion of governments' national sovereignty, the one from the U.K. and other nation-states of the world.

In the case of a young democracy that never considered shutting down the Internet and never did it, like Brazil, the cyber nationalism is also important, but in a very different way than the U.S. and the U.K. After the Snowden revelation of U.S. surveillance at a worldwide level, Brazil became a defender of the data protection of its own citizens and companies that circulates within the Internet. The Brazilian President at the time, Dilma Rouseff, emphasized the Brazilians' concern for protecting the information of their corporations because of their economic and strategic value (Harvey, 2011). Even more, Dilma Rouseff called the Snowden revelations 1) a situation of grave violation of human rights and of civil liberties for compromising data of individual citizens and, 2) of invasion and capture of confidential information concerning corporate activities, and especially of disrespect to national sovereignty (Rouseff, 2013).

Brazil called for the creation of new IXPs in the entire South American region to "retain" the data in the south and reduce the dependence from the U.S. IXP located in Florida. At the same time, Dilma Rouseff called to the international community to create any potential regulation over the Internet infrastructure with full respect to the rules of international law (Keating, 2013a). Within this context, the idea of cyber nationalism for Brazil is the protection of the data of its individual citizens, their private corporations and the government itself. These three elements in the context of NetMundial (A global multi stakeholder meeting on the Internet governance hosted by the Brazilian government in 2014) and the statements of President Dilma Rouseff are vital pieces of the survival of any nation-state.

In the case of hybrid regimes, cyber nationalism has a different, but at some extent the concept is like the one handled by Brazil. As I already explained in the case of Russia, the Internet in that nation state has its own identity: it has its own name, its own mascot and a set of laws that grant power to the government as much control as possible over the Internet infrastructure. The idea that another nation-state controls or can manipulate is unacceptable for the Russian government, moreover for the Vladimir Putin administration. In the same line, all data that belongs to the Russian population, government and industry must remain within Russian territory. With this purpose in mind, the Russian government created a legal framework that forces foreign companies to build servers within Russian territory and keep there the data of their citizens. The idea of a national Internet was taken to the extreme when the Russian government decided that the possibility of shutting down the Internet is an option with the solo purpose of protecting themselves from the U.S. and western nation-states (Keating, 2013b; Muggah, 2013).

4.4.1.5. What Remains: Political Factors

As it can be appreciated there are some points of coincidence between the regimes that shutdown the Internet or considered doing so, and the ones who did not: the fear of a cyberattack over the critical infrastructure, the use by Internet users of social network platforms or message systems during times of national unrest or public protest and claims of national sovereignty over the Internet. From a comparative point of view, these elements are the ones that remain as political factors for hybrid and democratic regimes to shut down the Internet.

4.4.2. Technical Factors (TF)

The technical factors referred to the crucial aspects a government may be able to manipulate and that can have access over industry and businesses. Technical factors are important because they define what companies and individuals may be able to do in practical terms. Table 08 details the main technical factors this project identified (Asmolov, 2015; Belousov, 2014; Bodner, 2014; Dolgov, 2015a, 2015b).

Table 08.- Comparison Technical Factors that enable Hybrid and Democratic Regimes to Shut Down the Internet or to Consider Doing So				
Factor / Nation-State	Internet Shut Down: Considered (C), Happened (H), None (N)	One or few ISPs Handles over the 70% of the Internet Subscribers	None IXPs, Few IXPs or IXPs under Government Control	DNS Poison: Use of non-traditional Alternatives of Action over the Internet Infrastructure
Russia	C		x	
Venezuela	H	x	x	
Turkey	N	x		x
U.S.	C	x		
U.K.	C	x		
Australia	H	x		
Mexico	N	x	x	
Brazil	N			

4.4.2.1. One or Few ISPs Handle Over the 70% of the Internet Subscribers

The conclusions of the cases under study are two: (1) between one and four ISPs handle over 70% of the Internet subscribers in hybrid and democratic regimes and, (2) only hybrid regimes have government-owned-ISPs. In terms of the role of the ISPs, I mentioned before that by stopping the service of one (or a few) ISP, the population served by that specific ISP, which previously had Internet access, would not have it anymore. Controlling ISPs is part of the process governments follow to shut down the Internet. As the evidence demonstrates, hybrid regimes and even consolidated democracies with few ISPs seem more willing to shut down the Internet or to consider doing so.

In terms of a specific comparison between a hybrid regime and a consolidated democracy, both Venezuela and Australia, have suffered multiple Internet shutdowns. Both nation-states also have a single ISP that handles over the 90% of the Internet subscribers. The Venezuela government

owns CANTV and the Australian government is the former owner of TELSTRA (Beijnum, 2011; Medows, 2012).

As depicted before, Internet shut downs in Venezuela referred to three different causes: 1) back in 2013, it was a response to a foreign attack to the communication platforms of the ruling party, 2) to control the dissemination of the information during the protests against the administration of Nicolás Maduro (concentrated in San Cristóbal, capital city of Táchira) and 3) an accident, when CANTV alleged that it had technical problems providing the service (El Universal, 2015; Hernandez, 2014; HwCol, 2014; Sainsbury, 2009).

In the case of Australia, this dissertation identified at least five Internet shutdowns in Australia between 2013 and 2016, however there are allegations that Telstra suffered at least four episodes only during 2016. In every single case, the explanation of Telstra is that there was either an accident, consequence of the hot weather or a human error (Diaz Hernandez, 2013; El Universal, 2015; Espinoza, 2015; Gomez, 2013; Mora, 2014). At this point, it is important to remember the critics of the private sector and the civil society in Australia about the Internet shut downs in that nation-state: they are not only very frequent, but the technical failures were never explained (Chester, 2016; Frankland, 2016; Kidman & Allen, 2012; Kiernan, 2016; Koerber, 2016; Stiles, 2016).

As a matter of fact, Greg Bader, the chief technology officer of iiNet (the second biggest ISP after TELSTRA) confirmed that the Australian government has the authority to enact a directive for the ISPs to stop connectivity and shut down the Internet. According Bader, this process would take around 30 minutes and involves shutting down equipment and routing because of the large amount of traffic that former-government-owned TELSTRA handles (Kidman & Allen, 2012).

In the case of the other democracies under study:

1. Although the U.S. has over 3,000 ISPs in its territory, four corporations, Comcast, Charter, AT&T, and Verizon, share about 76 percent of the 94.5 million internet subscribers in the U.S (Leskin, 2017). As a matter of fact, in 2016, it was believed that Charter could reach the 70% of the Internet subscriptions (Brodkin, 2016; Kafka & Molla, 2017). In a similar way, although the U.K. has around 3,000 ISPs in its territory, four corporations control most of the Internet subscribers in that nation-state: BT, TalkTalk, Virgin Media and Sky (BT, 2017; GOV.UK, 2012).
2. In the case of Mexico, the market is mostly controlled by three ISPs: América Móvil (also known as Telmex) controls 55% of Internet subscribers, Televisa handles the 22% and Megacable-MCM handles the 15% of Internet subscribers. These three ISPs handle over the 90% of the Internet subscribers and two of them over the 70%. This is a new balance within the Mexican market and is the result of a policy of the Mexican government to reduce the monopoly formerly controlled by Telmex (Lucas & Juarez, 2018; Martinez, 2018). More important is the distinction, despite of the fact that only three ISPs handle over the 90% of the Internet subscribers in Mexico, this nation-state never considered and never shut down the Internet.

4.4.2.2. No IXP, Few IXPs or IXPs Under Government Control

Controlling IXPs is the second step to attempt to shut down the Internet after controlling the ISPs. Not always is possible to control IXPs completely as they can have an international portion controlled from abroad. However, by controlling at least part of the IXPs, the connections

between ISPs are affected. Since IXPs facilitate the traffic among ISPs making it faster and fluid, by not having IXPs the Internet traffic (no matter how high the level of Internet penetration rate is) may become extremely slow and of poor quality (Zuckerman, 2015). The more IXPs a nation-state has, they will provide a faster Internet service than the ones that do not have them and the cost of the service decreases (ISOC, 2012; Villarroel, 2015).

At least one of the cases under study has no IXPs. The evidence in the cases under study comes from Venezuela and at to some extent from Russia (DCM, 2015). Venezuela has a high level of Internet penetration rate (over 60%), however it also has the slowest Internet in Latin America, the most expensive and of poorest quality (PCH, 2015, 2017). When is about an Internet shut down, just like I explained before, the lack of an IXP within Venezuelan territory facilitates the process. By lacking IXPs, if the Venezuelan government wants to act over the Internet infrastructure, they basically have to worry about controlling the ISPs, which is exactly what happened during the three episodes that nation-state suffered (CEPAL, 2016).

Differently from Venezuela, Russia has 29 IXPs. This would not be out of the ordinary, except for the fact that, the Russian government has an indirect control over those IXPs. In general IXPs are handled by private corporations (Coughlin, 2015; Dyn, 2014b); however, in the case of Russia, Rostelecom, a company with close ties to the government, mans all of them (Bodner, 2014). Before 2013, Russia's attempts to control the Internet were limited to securing government communications from foreign control, but that aspiration expanded to include the entire national Internet infrastructure (Dyn, 2012; Golitsyna et al., 2016; ISOC, 2012).

Again, a case apart comes from Mexico, a young democracy. Mexico has one IXP that functions partially; in practical terms, it is not very useful because ISPs are already very integrated. The integration started a few years ago when Telmex had a monopoly over the Internet users.

Despite of this situation, which increases the cost of the Internet service, Mexico never considered shutting down the Internet (Korsunskaya & Winning, 2016). As a matter of fact, this option was not even part of the discussion within the Mexican Internet policy debate.

4.4.2.3. DNS Poisoning

Controlling the DNS in any form can deprive most of the population from getting the information they want to access or uploading information they want to share in the Internet. As explained in the first chapters of this dissertation, one of the forms of acting over the DNS is by poisoning it and among all the cases under study, Turkey is the one that used this technique (Arreola, 2014; Terra, 2014).

On March 20, 2014, Recep Tayyip Erdoğan, at the time the 25th Turkish Prime Minister (and today's president), threatened to "root out" the social media because these platforms published wiretapped recordings that damaged the Turkish government reputation ahead of the local elections (Zmijewski, 2014). On March 21st, 2014, publicly manifested his dislike towards social media. On that day, Erdoğan ordered to block different sites and also to poison the Twitter DNS. In response to this situation, Turkish Internet users changed the settings in their devices to use Google DNS international providers like 8.8.8.8 and 8.8.4.4 or Level 3's at 4.2.2.1 and 4.2.2.2 (Rawlinson, 2014).

People painted the numbers in the walls in the street, so everyone could see them. Because of this political move, Twitter's popularity increased in Turkey but on March 22nd, 2014, the government decided to block directly the IP address of Twitter. On March 27th, 2014, YouTube's domain was also poisoned. On March 29th, the Turkish government also poisoned the Google IP

address. As a result of this, when Turkish Internet users asked a Google DNS server to connect to a YouTube's address, they got the IP address of a Turkish government site hosted by Turk Telecom (Sifir, 2014).

Despite of this disruptive policy, shutting down the Internet was never part of the discourse in Turkey. By poison multiple IP addresses, the Turkish government did it with a specific purpose: to control social media, which has become the "modus operandi" within its Internet censoring policy. Differently from Russia, Turkey had no interest in preserving the data of its citizens or to preserve any means of communication.

In Turkey, social platforms directly threatened the possibility that the incumbent party remains in power, during time of elections. In Turkey elections were going to be held a few days after the government poisoned the DNS in 2014, because the information disseminated in the social networks directly damaged the reputation of the AK party, Erdoğan's party. By poisoning the DNS, Turkey made clear that: 1) the ruling party is extremely concerned about remaining in power, like in Venezuela or Russia, and that 2) they have an infrastructure that can give them control over the DNS, a move very different from Russia and Venezuela.

4.4.2.4. What Remains: Technical Factors

In this section, the points of coincidence between the regimes that shutdown the Internet or considered doing so, and the ones who did not: the existence of one ISP or very few ISPs that handle over 90% of Internet subscribers (or at least a very big portion of it, like in the U.S.) and the existence of few IXPs, none or IXPs under control of the government. In the case of the U.S., it is important to be remember that, as mentioned before, although there are over 2,000 ISPs in its

territory, the market is dominated by four Internet service providers: AT&T, Verizon, Comcast and Charter (Ueland, 2017).

The case of the IXPs is a distinctive point of difference. Democratic regimes that shut down the Internet or considered doing so, have between 24 and 178 IXPs privately owned. Depending upon specific circumstances this number would be enough to guarantee speed and quality of the Internet traffic among ISPs. On the other hand, hybrid regimes lack IXPs, like Venezuela, or they are under government control, like in the Russian case.

From a comparative point of view, these elements are the ones that remain as strong technical factors between hybrid and democratic regimes.

4.4.3. Legal Factors (LF)

The legal factors referred to laws and regulations that affect businesses and individuals in a specific nation-state. It is expected that legal statutes change time to time (Zmijewski, 2014). This dissertation identified one legal factor common to all the cases under study, whether they are consolidated democracies or hybrid regimes: the existence of broad national security laws or telecommunication laws with unclear provisions about national security and the way governments should act. However, in the case of young democracies, there is an element that restrains governments to shut down the Internet: a specific legal or constitutional framework that protects the Internet infrastructure. Table 09 (see below) shows the comparison:

Table 09.- Comparison Legal Factors that enable Hybrid and Democratic Regimes to Shut Down the Internet or to Consider Doing So			
Factor / Nation-State	**Internet Shut Down: Considered (C), Happened (H), None (N)**	**Broad National Security Laws**	**Legal and/or Constitutional Restrictions to Shut Down the Internet**
Russia	C	x	
Venezuela	H	x	
Turkey	N	x	
U.S.	C	x	
U.K.	C	x	
Australia	H	x	
Mexico	N	x	x
Brazil	N	x	x

Authorities of the hybrid and democratic governments seem to agree in the fact that there is a group of laws that give them power over the Internet infrastructure, to the point of shutting down the Internet if a matter of national security is involved. These laws were mentioned previously when explaining each case. This chapter will provide specific opinions government authorities have about an Internet shut down when citing these laws:

1. Australia: Telecommunications Act of 1979 and amendments of 1997 and 2003

   According to the provision 581 of the statute, the attorney general (after consultations with the Prime Minister and the Minister of Telecommunications) is entitled to request ISPs to stop providing Internet service under circumstances "prejudicial to security" (PESTLE, 2015b, 2017)

2. U.S.: Telecommunications Law of 1934 and amendments of 1996. Citing the war powers of the president, during the discussion about the new 2012 Executive Order of the White House, Phillip Reitinger (at the time the head of the DHS) clarified that although the executive order does not contain a provision to shut down the

Internet, control over the telecommunications is a prerogative of the president. Such prerogative will be used according the specific case (Keane, 2012a, 2012b) U.K.: Communication Act of 2003. According to the section 132 of the Communications Act of 2003, OFCOM, the "Independent regulator and competition authority for the United Kingdom communications industries," can request to any U.K.-based ISP the suspension of the service to preserve the "public order" or in case of a massive cyber-attack. OFCOM has the authority to act on behalf of one of the ministers, most likely the minister of culture, who would be the one who has legal authority to "shut down the web" (Phillip Reitinger et al., 2011). Along with section 132 of the Communications Act of 2003, the part 2 of the Civil Contingencies Act of 2004 also would give to the executive branch legal authority to request to the ISPs the suspension of the Internet service. According to part 2 of the Civil Contingencies Act, the executive branch is entitled to create emergency regulations if the U.K. faces a national security threat (Hardings, 2011; Marsden, 2011).

At this point it is important to make a distinction between the U.S. and the U.K. law. Differently from the U.S. law, the U.K. law requires specific identification of the networks concerned and compensation for loss or damage to the businesses impacted if the Internet was shut down. Also, differently from the U.S. law, ISPs are not required to follow immediately an order of the administration. The law requires to serve a network operator with a suspension notice and the ISP may actually ignore it (Hardings, 2011; Marsden, 2011).

3. Russia: "Blitzkrieg laws" over the Internet infrastructure, 2002-2016. This is not a law but a big group of laws the Russian government enacted between 2002 and

2016 with the purpose of controlling completely the Internet infrastructure. Although Russia does not have a specific law that allow the government to shut down the Internet, the administration of Vladimir Putting has created these set of laws between 2002-2016 (when he was either the president or prime minister) to gain complete control over Russia's Internet infrastructure. As understood by policy makers and academics in Russia, these measures only prepare the RUNET infrastructure to be able to be shut down when the government considers to do it (Winder, 2011)

4. Venezuela: The Law of Social Responsibility and Quality of the Television in Venezuela of 2005 (RESORTE). RESORTE forbids content considered "offensive," "violent," "disrupt public order," "disown pubic authorities," and "Induce homicide". It is the government authority (the regulator in this case), the one to decide when the content falls into the previous categories. Actions to take also are entirely decision of the executive branch and they may include shutting down the Internet (Asmolov, 2015; Duffy, 2015; Krieger, 2015)
5. Turkey: The Law 5651, "Law No. 5651 on Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting," gave power to the Turkish regulator, TIB, in order to 1) block Internet access and 2) collect Internet traffic accessing IP numbers, subscriber numbers, subscription information form the ISPs, the type of service and the amount of data used (Finol & Espinoza, 2015; Gonzalo, 2010). The enactment of the law 5651 is very aligned with all the Russian laws to control the Internet infrastructure (Kizilkaya, 2014;

trend, 2014). The difference however is that shutting down the Internet has never been part of the Turkish policy debate or government activity

The last part of the legal analysis comes from the young democracies, Mexico and Brazil. According their own statements, these regimes do exercise activities of control over the Internet content for drug dealing prosecution in the case of Mexico (OpenNet, 2013; OSCE RFOM, 2009; Zeldin, 2014) and for privacy purposes or for prosecution purposes in the case of Brazil. In the case of Brazil, social networks have been blocked in the past because of a court ruling (Merkelsson, 2010; Norzagaray Lopez, 2008). However, the Internet shut down is not in their debate and in cases like Brazil, the idea of using this extreme measure of control has been clearly denied (Grossi, 2014; Olukotun & Pallero, 2016; Reuters, 2007). What these two regimes have in common is the existence of a legal or constitutional regime that protects at some extent the Internet infrastructure.

As referred before, the Brazilian Congress enacted what is known as the Brazilian Internet bill of rights, the "Marco Civil" legislation. Marco Civil, also known as the "Internet bill of rights" protects privacy online and the network neutrality (Carpes, 2012). Marco Civil does not contain provisions declaring the Internet a human right, but it was built on the approach of Mr. Frank La Rue (the U.N. Special Rapporteur on Freedom of Expression between August 2008 – July 2014) of having a framework for human rights within the Internet. In this regard, Marco Civil was designed on the idea that the Internet should be an open, affordable and accessible space and never should be shut down. This is the reason why Marco Civil does not contain generic ban provisions regarding content in the Internet. When is about national security, Marco Civil does not address any issues related to this subject (Moncau & Mizukami, 2014; Peralta, 2014). In Brazil, any activity related to national security is regulated through a national strategy on cyber security prepared to address the organize crime as a major threat to Brazilian Internet and focusing on

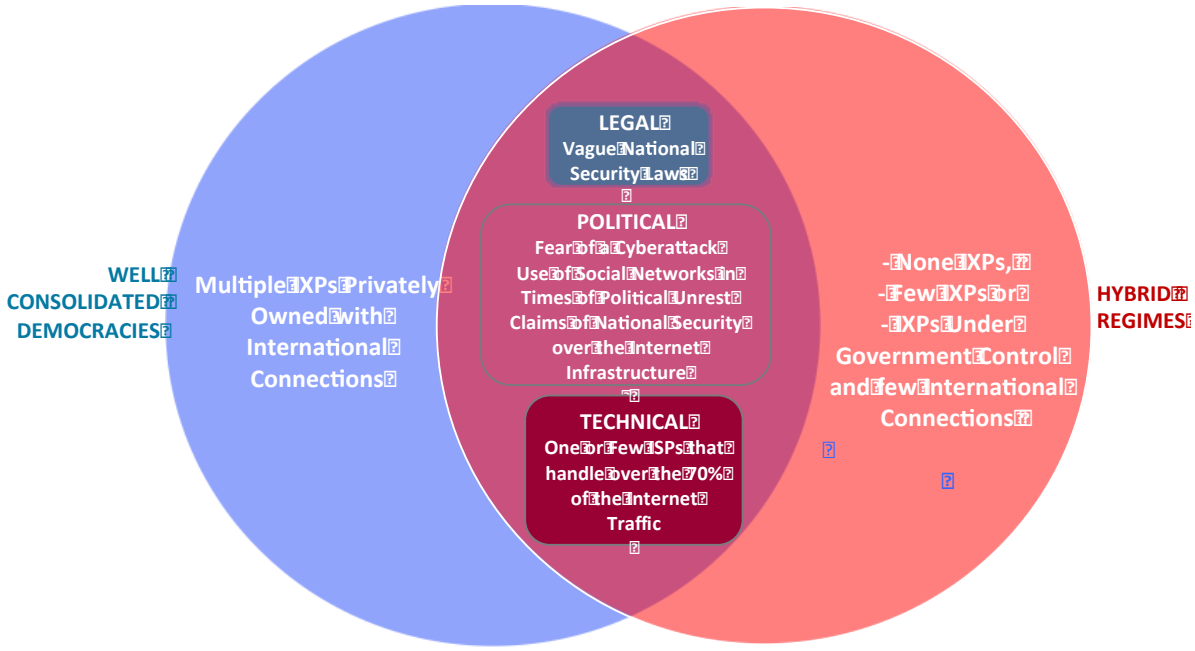
military solutions in cases of warfare. However, in any case an Internet shut down was never address or considered by this legislation (Rossini, Cruz, & Doneda, 2015). In the case of Mexico, a modification of its constitution in 2013, gives to the access to Internet the condition of human right, without limitation. In accordance with the Mexican government opinion and legal opinions, shutting down the Internet would be an unconstitutional action. Therefore, no laws (not even national security laws) can regulate or accept the possibility of shutting down the Internet (Diniz, Muggah, & Glenny, 2014).

4.4.3.1.What Remains: Legal Factors (LF)

The common characteristic of all the cases under study is the existence of vague or broad national security laws. From a comparative point of view, this element is the one that remain as legal factor for hybrid and democratic regimes to shut down the Internet. On this matter, it is important to precise that this is a common characteristic of national security legislations all over the world. The concept is never clarified by a national legislation and this is purposely done so consecutive administrations can clarify the concept of national security according the needs and changes of their time.

Figure 20 shows a graphic representation of the elements I identified as political, legal and technical factors that enable hybrid and democratic regimes to shut down the Internet for comparison purposes.

Figure 20.- Comparative Graphic: Political, Legal and Technical Factors that enable Democratic and Hybrid Regimes to Shut Down the Internet



5. Discussion

This chapter details the most important issues this dissertation identified when talking about the policy known as “Internet shutdown”. These issues intent to enrich the Internet governance debate about Internet shutdowns, the importance of analyzing this subject within the sphere of democratic and hybrid regimes and, the role of national security policies when framing this extreme policy over Internet infrastructure.

The next chapters will provide an analysis of each one of the aspects previously listed and will highlight the importance of the securitization theory and a comparative case study research method to analyze the results.

5.1. Context: The Internet Kill Switch, why this Subject is Important

When the Internet in Egypt vanished from the international Internet traffic in 2011, the world was aware by the first time that such disruptive policy could be accomplished by an authoritarian government. The term used to describe this government action was called “Internet shutdown”. Same policy was debated at a legislative level in the U.S. between 2009 and 2011. However, it is not very well known that the first time the Internet was shut down was in Nepal in 2005.

Since then, this disruptive policy has become more frequent and has been used constantly for different reasons. Most cases include authoritarian regimes trying to fight against public protest of their own citizens. These authoritarian regimes constantly claim that the goal of the protesters is destabilizing the incumbent government and therefore, to destroy the administrative structure of

the nation-state. Hybrid regimes also claimed similar scenarios in their own territories. By facing similar circumstances, hybrid regimes like Venezuela, also executed Internet shutdowns.

This is however, just one side of the problem. Differently from what most people may think, the policy of shutting down the Internet, as controversial and extreme as it is, has also been debated at a political, legal and academic level by well-consolidated democracies, such as the U.S. the U.K. and Australia. Young democracies like India even approved an administrative framework to allow the government to shut down the Internet under reasons of national security. The debate in all those cases focused in the existence of national security circumstances, but the debate also will put on the table two things: (1) The existence of multiple concepts of national security when analyzing an Internet shutdown and (2) The existence of similarities in the national security discourse of hybrid and democratic regimes.

5.2. Different Views of What an Issue of National Security is

As mentioned many times in this dissertation, national security is a theoretical concept that is framed under specific circumstances in a specific time by the government of a nation-state (Richards, 2012).

The security discourse in all regimes under study claims reasons of national security to shut down or consider shutting down the Internet. However, there are different views of what an issue of national security that may prompt an Internet shutdown is. While well-consolidated democracies address as national security the protection of the critical infrastructure, hybrid regimes are concern about the flow of data and national protests.

Nevertheless, it is important to say that, although these are mainly the reasons that those governments claim, not everything is black and white. Well-consolidated democracies are also worried about national protests and hybrid regimes are also concern about the protection of the critical infrastructure. The next paragraphs contain an overview and explanation about each one of these concepts.

5.3. A Conceptual Problem: Two Views of What an Internet Shutdown is

This project has defined the term "Internet shutdown" as the attempt to stop all Internet activity within the borders of the territory of a nation-state. However, within the Internet governance debate there are different definitions. As mentioned at the beginning of this project, the Internet Society (ISOC) and an organization named Access define the term "Internet shutdown" as "intentional disruption of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location often to exert control over the flow of information" (ISOC, 2017, para.4). ISOC also clarifies the types of Internet shutdowns as a total shutdown (what I call and Internet kill) switch and a partial shutdown (episodes of censorship) (ISOC, 2017).

As I developed more deeply in the first chapter of this dissertation, I agree only with the first part of this definition. An Internet shutdown is such when it affects specific elements of the infrastructure and services that support Internet access, like ISPS, IXPs, fiber optic cables, the DNS and the BGP. In this regard, an Internet shutdown target is not a specific application, but the entire infrastructure of the Internet. As the same definition of ISOC states itself, when talking about specific applications, I refer to episodes of censorship (ISOC uses the words "content blocking"),

whether they are technical blockings, search result removals or take down. Analyzing episodes of censorship is also very usual in the Internet governance debate and they are more common and constants than Internet shutdowns.

As an additional point regarding the distinction in the different views of what an Internet shutdown is, I must bring attention over some reports of the Brooking Institution (West, 2016) and the Global Network Initiative (GNI) (Deloitte, 2016). Both reports pointed out to the economic cost of the Internet shutdowns for a nation-state. This is another example of the problems in the distinction, because these reports don't explain the difference between the costs caused for disrupting the flow of data of specific applications and the disruption of the entire Internet infrastructure.

5.4. The Importance of Identifying the infrastructure and services that support Internet access

By using the elements of the TCP/IP protocol, this dissertation provided some parameters to define what an Internet shut down is and how it can be achieved, in a way to make a clear distinction from censorship episodes. This point is extremely important because, by having a clear concept of an Internet shutdown as an extraordinary measure, it was possible to build our research design through: 1. The use of a theoretical model, the securitization theory of the Copenhagen School and 2. The use of a comparative case study.

As mentioned previously during this dissertation, shutting down the Internet is a complex process that involves multiple stakeholders as the different elements of the TCP/IP protocol are

owned or handled by different entities. As mentioned, the elements to control to achieve an Internet shutdown are as follow:

1. ISPs are the first stakeholder to be controlled. If these service providers cannot perform their activities, the population they serve will no longer have Internet access (Beijnum, 2011; Medows, 2012)
2. In the case of the IXPs, their presence is fundamental to keep a fluid traffic of the Interne packets and they also may provide international connections (Beijnum, 2011; Medows, 2012).
3. Internet cables facilitate over 99% of the Internet traffic (Madori, 2015)
4. DNS, the protocol that translates the host names into IP addresses (Vaughan-Nichols, 2011; Wang, 2003)
5. BGP is the routing protocol that shares the master routes of the Internet. In this way, the BGP makes it possible for ISPs to connect to each other and for end-users to connect to more than one ISP

Achieving an Internet shutdown means controlling all these elements, and therefore, national security policies must be oriented to control each one of these elements if the goal of a government is shutting down the Internet. This is a much more difficult task than only controlling specific applications.

5.5. Use of the Securitization Theory

The securitization theory of the Copenhagen school, also known as securitization theory, focuses on the analysis of one of the most important pieces of the justifications to achieve an

Internet shutdown: the national security discourse. According to the securitization theory, the discourse is the process of taking an issue from a politicized, or even non-politicized stage, into the security domain (Buzan, 1998; Dunn Cavelty, 2008). According to the terms of the theory, the study of securitization aims to gain an understanding of who securitizes (the actor) which issues (the threat subject), for whom or what (the referent object), why (the intention and purposes), with what results (the outcome), and under what conditions (the structure) (Buzan, p.32,1998)". Also, according to the theory, the securitizing agent builds a speech to convince an audience that an extreme measure must be executed to protect the referent object, which is also the national interest (Buzan, 1998).

Previous academic work has used the securitization theory from two perspectives: 1) to analyze U.S. policies that govern cyberspace since the attacks of September 11, 2001 (Dunn Cavelty, 2008), and 2) to analyze other nation-states securitization policies over diverse non-Internet-related issues.

This dissertation used the securitization theory of the Copenhagen School to analyze the speech around Internet shutdowns, as a policy implemented or considered by democratic and hybrid regimes to protect the national security of their nation-states. The use of this theory allowed us to identify similarities in the rhetoric of the speeches of hybrid regimes and well consolidated democracies. This means that, at a rhetorical level, limits between hybrid and democratic regimes national security policies are blurry when it comes to an Internet shutdown. There are similarities in the arguments of both types of regimes. The use of the securitization theory also allowed us to identify different referent objects (the element to be protected in terms of the theory), a concept also identified as the "national interest". The national interest is important because is that thing

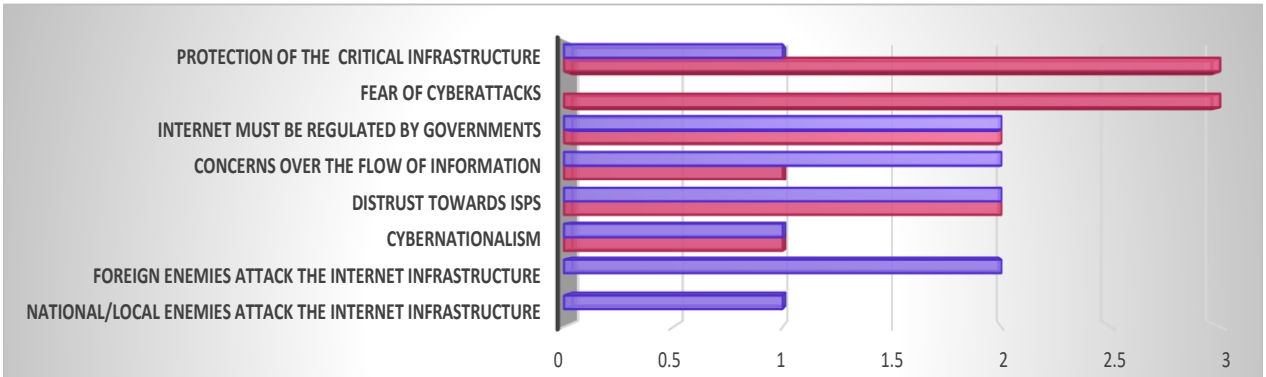
that must be protected in order to preserve the survival and stability of a nation-state (Richards, 2012). The referent object is the focus of every national security policy.

Additionally, the securitization theory also allowed us to examine and identify the audience that securitizing agents intend to address. In the terms of the theory, the audience must be convinced that an extreme measure, such as an Internet shutdown, is necessary to protect the referent object or national interest. This dissertation concluded that the importance of the audience in the case of Internet shutdowns is related to: 1) their capacity to act so the Internet can actually be shut down, this is the audience that must act and has the means to shut down the Internet and 2) their ownership of that thing the government wants to protect, that thing that is portrayed as the national interest, even if this audience cannot or refuses to shut down the Internet.

5.6. Similarities in the Rhetoric about Internet Shutdowns between Hybrid and Democratic Regimes

As mentioned before, findings show that there are no clear and "sharp" distinctions between the justifications why hybrids and democracies shutdown the Internet or consider doing it. Figure 22 (see below) shows a representation of the similarities and differences in the speech of these two types of regimes. The next paragraphs will provide an overview of the similarities and the meaning of each one.

Figure 21.- Comparison Between the Elements of the Security Discourse (Securitization Speech) in Democratic and Hybrid Regimes



	National/Local enemies attack the Internet infrastructure	Foreign enemies attack the Internet infrastructure	Cybernationalism	Distrust towards ISPs	Concerns over the flow of information	Internet must be regulated by Governments	Fear of cyberattacks	Protection of the Critical Infrastructure
Hybrid	1	2	1	2	2	2		1
Democracies			1	2	1	2	3	3

Hybrid Regimes (2) Venezuela and Russia
Democratic Regimes (3) Australia, U.K., U.S.

In this graphic I count the number of cases per element of the security discourse. The "Y' axe contains the element of discourse, while the "X" axe contains the numbers of nation-states (democracies and hybrids) under study that used this element in their speech. In this way I could compare how many regimes cited an element. In the next paragraphs I will provide an overview of the way these elements interact. The order of the elements corresponds with the frequency I identified them in the discourse. I also will explain differences among some of these concepts.

5.7. Cyberattacks (Cyber Pearl-Harbor) and the Protection of the Critical Infrastructure

The critical infrastructure is vital for the survival of any nation-state in the world, democratic or hybrid regimes. Its protection is also a matter of constant concern, especially in times when cyberattacks have increased (Seals, 2018). After the attacks of September 11, 2001, the different systems of the critical infrastructure were interconnected through the Internet, which eventually became a vulnerability because if one sector is under attack the rest may be affected too. Being this the situation, any national security policy over the Internet infrastructure must include the protection of the critical infrastructure (Radvanovsky, 2006).

The interconnection of the critical infrastructure was a decision adopted by hybrid and democratic regimes and today is also a matter of concern for both (Astakhov, 2016; MacKinnon, 2012; Pynnöniemi, 2012a, 2012c). This is an argument conveyed in the rhetoric of all the regimes analyzed in this case study. The cyberattack that can damage greatly the critical infrastructure is described as one of great magnitude, reason why well consolidated democracies called it “cyber Pearl Harbor”. However, neither democratic nor hybrid regimes can establish some parameters to identify a cyber-Pearl Harbor; in other words, they don’t know how to characterize this massive cyberattack.

5.8. Internet must be regulated by Governments: Applying Cybernationalism to the Internet Infrastructure

Nation-states under study have pretensions to create national regulations over the Internet infrastructure. Democratic regimes agree on the fact that the Internet must be regulated by their governments, without meddling from the international community (Krieger, 2017; LeMay, 2012). Similarly, in the case of Venezuela and Russia, both regimes also call for an absolute national regulation.

Hybrid regimes created one or many laws to control every single aspect that is relevant for the government administration, such as the flow of information, child pornography, intermediaries' responsibility, data storage, terrorism, bloggers' activity and anonymity. While Russians created different legal bodies named as "Blitzkrieg laws" over the Internet infrastructure, Venezuelans decided to amend the body related to the telecom infrastructure, the Law on Social Responsibility in Radio, Television and Electronic Media (RESORTE Law).

All these Russian attempts to control the Internet infrastructure were taken to an extreme at the end of 2017. By then, Russia announced its intention of creating an independent Internet for the BRICS[30], developing for the purpose a parallel and independent DNS system (Macdonald, 2017).

Although controversial, well consolidated democracies have had similar attempts to control the Internet infrastructure, but not all them became legal statutes like in hybrid cases. In any case, after 2001, well consolidated democracies also drafted bills to give governments more control over the Internet infrastructure. In the U.S. the debate about the securitization of the

[30] The acronym BRIC was publicly known in 2001 in a report written by Goldman Sachs economist Jim O'Neill. At the time, the four nations it referred made up just 8% of the world's total economy. The term initially included Brazil Russia, India and China. Later, South Africa also would be included and the term would change from BRIC to BRICS (Timmons, 2015).

cyberspace started (which included the Internet shutdown bills discussed in previous chapters). Additionally, the Australians tried to pass at least three white papers (the equivalent to U.S. bills) to give more control to the government over the critical infrastructure, created a blacklist of websites, changed twice the cybersecurity strategy and amended the telecommunications law to fight against child pornography. Like the Russian strategy, in 2015 the Australian parliament changed the telecom law to force companies to retain Internet users' records for two years and a court determined that Google was liable as a secondary publisher in a defamation case.

In this context of overwhelming production to control the Internet infrastructure, hybrid and democratic regime discussed or executed an Internet shutdown.

5.9. Concerns over the Free Flow of Information and Social Control Purposes

The free flow of information is a matter of concern for democracies and hybrid regimes, and, although controversial, justifications also overlap. In the case of Venezuela, concerns about the flow of information without any filter or control was first expressed by late President Hugo Chavez. Back in 2010, the Venezuelan government did not exercise so much power over the social networks, but Hugo Chavez blamed them because he claimed that individual citizens were posting whatever they wanted even if it was not true. According to Chavez this disinformation had as a purpose to create instability within his administration. In defense of his efforts to curtail Internet access, Chavez claimed that every nation-state should apply its own rules over the Internet (Chinea & Daniel, 2010).

British authorities had similar concerns during the London riots in 2011. They were certainly worried about the way information circulated by the protesters, while they were not able

to control, oversee it or stop it. If they did not shutdown the Internet was only because of the possible international repercussions of being compared with authoritarian practices (Williams, 2011). At some extent similar concerns are present in the U.S. during the BART episode, when the phones of protesters were silenced on the grounds of national security and safety. The content of the alleged mechanism to silence protesters and that may shut down the Internet, SOP 303 (an emergency wireless protocol), was never made public (EPIC, 2015).

In a different scenario, the Russian government is concerned over the flow of information that may compromise the data of the government itself or the data of the Russian citizens. As a matter of fact, this is the main argument for two potential scenarios related to an Internet shutdown: 1) a Russian government doing: to implement a shutdown of RuNet when the nation-state faces a national security threat , or 2) foreign enemies doing: to be prepared in case the U.S. and its allies attempt to attack RuNet and cut it off from the rest of the international Internet traffic (MacAskill, 2014; Russia Beyond the Headlines, 2015; Zavyalova, 2014).

5.10. Distrust towards ISPs

ISPs are an important element of the TCP/IP protocol, the first one to control if a government wants to shut down the Internet. This also manifests the importance of its role within the Internet ecosystem and the Internet governance debate.

The speech of both regimes, well consolidated democracies and hybrids, shows the lack of trust towards ISPs as providers of the Internet service. In case of Australia, Minister Conroy declared publicly what he considered the lack of cooperation from Australian ISPs when adopting Internet policies. He was referring to a specific censorship policy the Australian Parliament was discussing at the time (LeMay, 2010b). At the same time, the Venezuelan government declared its

distrust toward ISPs and made them liable as part of the process of information flow and include them in the law of social responsibility over the telecom infrastructure (Gonzalo, 2010; LeMay, 2010a, 2010b; YouTube, 2014).

Additionally, and more similar are the Russian and U.K. policy when it comes to the communications within their territories. Russia created legislation that forces ISPs to 1) store all information they process and keep it available to be reviewed by Russian authorities when required and 2) keep censoring attributions for the Russian regulator at its own discretion (Duffy, 2015). On the other hand, since 2009, ISPs in the U.K. are forced to keep information about every electronic mail sent or received in the U.K. for a year (A. Crawford, 2009).

5.11. Foreign Enemies Attack over the Internet Infrastructure

Differently from previous considerations, “foreign attacks” over the Internet infrastructure are a matter of concern explicitly for hybrid regimes. While well-consolidated democracies talk about attacks over the Internet infrastructure in a general way, hybrid regimes focus in the character of “foreign”.

The concept of a “foreign” enemy (without distinction of the entity, whether is a government, corporation or individual) belongs only to the hybrid speech (Belousov, 2014; Venprensa, 2013). This rhetoric, although not new, became more powerful after the Snowden revelations, as a constant for hybrid regimes of blaming foreign powers for their problems. Russia would talk about the “unpredictable west”. The foreign enemy can be either another regime or government administration, such as the U.S. in the case of Russia, or an unknown individual like in the case of Venezuela (Belousov, 2014; MacAskill, 2014; noticias24, 2013).

5.12. National/Local Enemies Attack over the Internet Infrastructure

Local enemies attacking the Internet infrastructure are explicitly referred to in only one case of a hybrid regime, Venezuela. That nation-state has been in turmoil since 2013 and, in at least one episode of an Internet shutdown at the beginning of 2014, local authorities blamed "internal enemies," specifically political rivals of the current administration as responsible for this act. This episode is the result of violent protests in the city of San Cristobal, where the Internet service was suspended for several days (Delgado, 2014; Mora, 2014; SOSVenezuela2014, 2014).

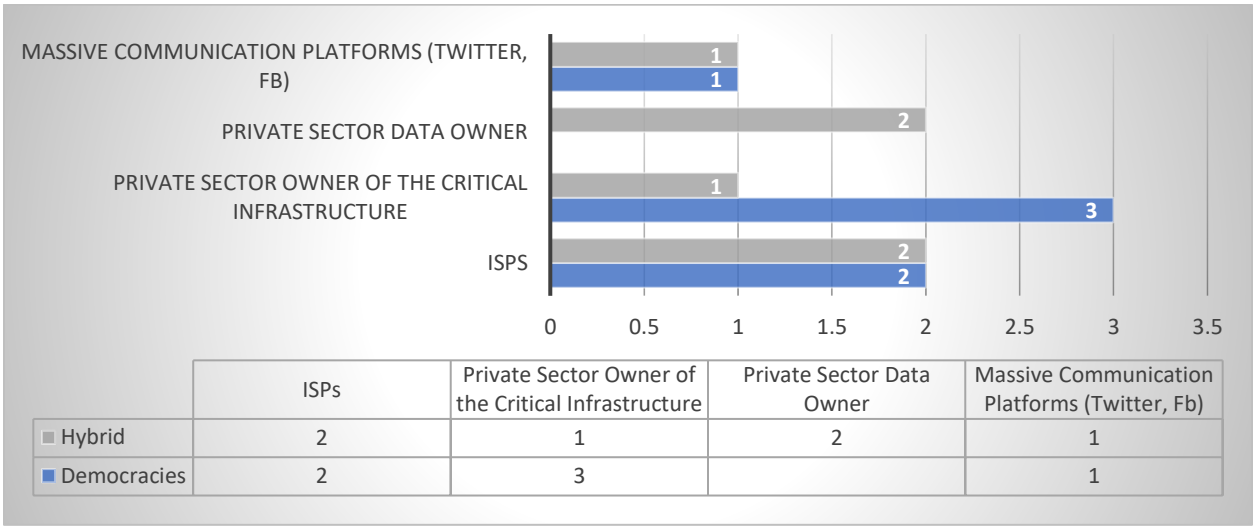
5.13. Similarities in the Audiences

As analyzed previously, according to the terms of the securitization theory, audiences can either: 1. Challenge the securitizing actor's presentation of what should be a national security issue, or 2. They provide support to the securitizing move (Côté, 2016; Vuori, 2008). In any case, audience(s) are important because they can provide what the securitizing actor needs to accomplish or reformulate the securitization process (Vuori, 2008). In these terms, audiences have the capacity to accomplish what the securitizing agents want (they have the means to do it) or differently, audiences may not share some basic assumptions with the securitizing agent in order to buy the securitizing speech (Campbell, 2009; Côté, 2016; Vuori, 2008).

One of the conclusions of this dissertation is that the audience is always the private sector, but exactly who in the private sector is an actor, will change depending on the type of context and regime.

Figure 22 (see below) shows a representation of the similarities in the audiences democratic and hybrid regimes want to convince that an Internet shutdown is necessary. Like in the previous graphic, the "Y' axe contains the specific audience to address, while the "X" axe contains the numbers of nation-states (democracies and hybrids) under study that addressed these audiences in their speech. In this way we can compare to whom democratic and hybrid regimes try to convince that an Internet shutdown is necessary to protect the national interest.

Figure 22.- Comparison Between Audiences Democratic and Hybrid Regimes Intent to Convince that an Internet Shutdown is necessary



	ISPs	Private Sector Owner of the Critical Infrastructure	Private Sector Data Owner	Massive Communication Platforms (Twitter, Fb)
Hybrid	2	1	2	1
Democracies	2	3		1

Hybrid Regimes (2)	Venezuela and Russia
Democratic Regimes (3)	Australia, U.K., U.S.

The main audience for consolidated democracies is the one that owns and handles the critical infrastructure, because this is the national interest, the element to protect to preserve the survival of a nation-state. The protection of the critical infrastructure became critical after the attacks of 2001 in the U.S. because the critical infrastructure is interconnected by the Internet.

When it is about the Internet shutdown, they need the support of the private sector to achieve a successful national security policy because the private sector is capable of legitimate (if they agree) the security discourse. Moreover, within the owners of the critical infrastructure, there are the owners of the Internet and telecom infrastructure, and their help and support are needed to any attempt to shut down the Internet. In concrete, well consolidated democracies, have mentioned that their legal statutes should be able to command ISPs, as the first audience to address, to shut down the Internet by command of the executive branch (CNN, 2010; Hardings, 2011; LeMay, 2010a).

In case of hybrid regimes, they have as a targeted audience the private sector that controls the information they cannot control and that they would like to handle. References in Venezuela and Russia have the same pattern: initially they make ISPs accountable because they have a hand in the control of what is posted and how the information flows, which makes them legally responsible. However, IPSs are just the first block in the chain. Governments want to control the rest of the Internet stakeholders that handle the Internet infrastructure. These includes IPSs they don't own and the international connections they handle. Moreover, they also want to control the rest of the private sector in the information flow, social networks and private companies located abroad.

Social network platforms such as Facebook, Twitter or similar have been used to circulate information in some way governments cannot control. Social network platforms were accused of spreading false information by hybrid regimes like Venezuela and, they also were accused of spreading "ill information" by well consolidated democracies like the U.K. In both scenarios there is an important element, governments lack of control over the flow of information that circulates within the social networks. Social networks cannot achieve an Internet shutdown, as a matter of

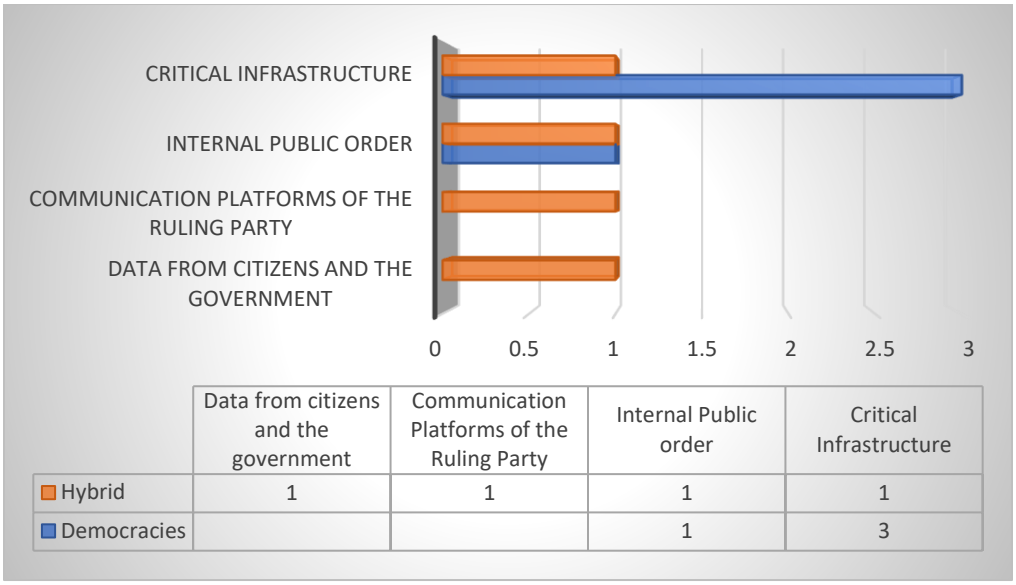
fact they tend to be against this policy. However, they are a key element framing the securitization policy because of their solo existence. Social network platforms own that thing the government wants to control: the flow of information, either because they consider it false or because the government wants to stop it.

5.14. Different Views of the Referent Object

As mentioned in previous chapters, theoretically speaking, national security is a set of policies a nation-state develops to protect what they consider the national interest, that thing that needs to be protected to preserve the survival of a nation-state. Different national security policies exist because there are different conceptions of what the national interest should be (Richards, 2012). In terms of the Copenhagen securitization theory, the national interest is called a referent object.

Figure 24 (see below) shows a representation of the different referent objects in hybrid and democratic regimes. The "Y' axis contains the different referent objects this dissertation identified, while the "X" axis contains the numbers of nation-states (democracies and hybrids) under study that used this element in their speech. In this way we could compare how many regimes cited an element. The order of the elements corresponds with the frequency they are used in the security discourse.

Figure 23.- Comparison Between the Referent Objects in Democratic and Hybrid Regimes



	Data from citizens and the government	Communication Platforms of the Ruling Party	Internal Public order	Critical Infrastructure
Hybrid	1	1	1	1
Democracies			1	3

Hybrid Regimes (2)	Venezuela and Russia
Democratic Regimes (3)	Australia, U.K., U.S.

5.15. Critical Infrastructure

Consolidated democracies consider the critical infrastructure the main object of their national security policies, and its protection frames the elements of the securitizing speech of those governments. In the view of these governments, the destruction or misuse of a critical infrastructure asset would have an impact on the health, safety, welfare, or economic security within a nation-state (Radvanovsky, 2006). As such, it requires protection, including an extreme a measure as shutting down the Internet. As a matter of fact, the term Cyber Pearl Harbor, a potential massive cyberattack over the critical infrastructure, is a constant fear policy makers address when they create national security policies (H. Farrell, 2013). The critical infrastructure has been the main object of protection and point of debate during the last eighteen years in the national security policies of the U.S. government, especially when it is related to the Internet (Chalfant, 2017; Dunn

Cavelty, 2008). The U.K. and Australia have very similar national security policies focused in the critical infrastructure (HM Government, 2016; Senator Stephen Conroy, 2008).

For hybrid regimes, specifically Russia, the critical infrastructure is also a very important part of their national security policies. However, the levels of concern are addressed differently from two different points of view: ownership and potential threats.

As mentioned many times in this document, the main concern for democratic regimes is the existence of a cyberattack (a.k.a. cyber Pearl Harbor). Concerns of the democratic governments are such because the critical infrastructure is mostly owned and controlled by the private sector, not only the government. Therefore, the private sector always must be included as part of every national security policy.

In hybrid regimes the situation is different. In Russia, the control of the critical infrastructure is mostly in hands of the government or in hands of private entities with close connections to the government or under its control. Also, differently from the democratic approach, the Russian government has three focuses of concern (instead of only one): terrorism, climate change and cyberattacks. Nevertheless, the critical infrastructure is as important for hybrid regimes as it is for democratic ones. That is the reason why the Russian government developed and is constantly updating a national security policy on this subject (Pynnöniemi, 2012b).

5.16. Internal Public Order

Part of the academic literature has suggested that the governments of hybrid and authoritarian regimes may try to disrupt the Internet traffic to prevent political mobilization and public protest (Howard et al., 2011; Michaelsen, 2016). However, this research has shown that

democratic regimes also may try similar policies when facing a public protest that goes beyond what authorities can handle. This was the case during the riots of London in 2011. Although the initial government position of shutting down the Internet moved to a softer one of shutting down the social networks, the purpose remains the same, what the British government was aiming to protect was the internal public order (Williams, 2011). As mentioned before, public order refers to the operations of a society and the ability of its people to function efficiently or at least in the pre-established order or a specific status quo.

When the British government initially considered to shut down the Internet, they did it to preserve the internal public order. According to that government mindset, the internal public order was threatened by the split of information within social networks in a way the government could not control.

A very similar approach was adopted by Venezuela in 2014 during the protests in the city of Táchira, when the Venezuela government blamed the social platforms as well for spreading the violence in a way they could not stop. Differently from the British case, the Venezuelan government also blamed the protesters for damaging the Internet infrastructure (Mora, 2014; Noticias24, 2014).

5.17. Communications Platforms of the Ruling Party

Although the academic debate has focused in the importance hybrid regimes put on the flow of information, this has never been considered as a reason to shut down the Internet. This dissertation identified the protection of the communication of the means of the ruling party as a

reason to do it. The reason lies in the governments' loss of control over the spread of information online.

Venezuela shut down the Internet twice to protect public sites that, although should remain neutral, have been used as communication platforms by the government. This occurred at the time that also other social network platforms were hacked, specifically the Twitter accounts of Nicolás Maduro and the ruling party. In these conditions these platforms present information that was false or ridiculed Nicolás Maduro. The government was not able to control any of the things that were made public. Moreover, they lost the capacity of communicating whatever they wanted to the rest of the world.

In the first episode, the presidential elections of 2013 and the protests of 2014, the Venezuela government shutdown the Internet and blamed third parties because of this situation (Diaz, 2014; El19, 2013).

5.18. Data from Citizens and the Government

As analyzed before, after the Snowden revelations in 2013, the Russian administration became highly concerned about the possibility that foreign governments access data from Russian citizens and the Russian government. The possibility of this foreign access is an essential element of the securitizing speech of the Russian national security policy to justify an Internet shutdown. In this regard, the Russian approach contemplates the policy of an Internet shutdown in a way the Internet governance debate has not done yet.

First, Russians propose to shut down the Internet to protect their critical infrastructure from what they call "the unpredictable" actions of the U.S. government and their allies, or "the

unpredictable west". In other words, they fear that foreign powers have access to the government and citizens' data. However, the novelty comes from a defensive approach. The government must be able to disconnect RuNet from the rest of the international d, but also must be ready to face a scenario where foreign powers disconnect RuNet as a form of foreign cyberattack. Alleged cases of an Internet shutdown because of a foreign attack are not many. I identified two cases, North Korea and Syria, although in none of them there is evidence. The Russian government seems to be preparing for a potential case like this, although not much detail has been revealed.

5.19. Beyond the Theoretical Framework: The Use of a Comparative Case Study

The theoretical framework of the Copenhagen School allowed us to analyze the rhetoric behind the use of a disruptive policy like an Internet shutdown. However, rhetoric and real causes and contexts to apply a policy are not necessarily the same. This is the reasons why besides studying the speech by hybrid and consolidated democracies, I also analyzed the political, technical and legal factors that enable a hybrid regime or a democratic one to shut down the Internet.

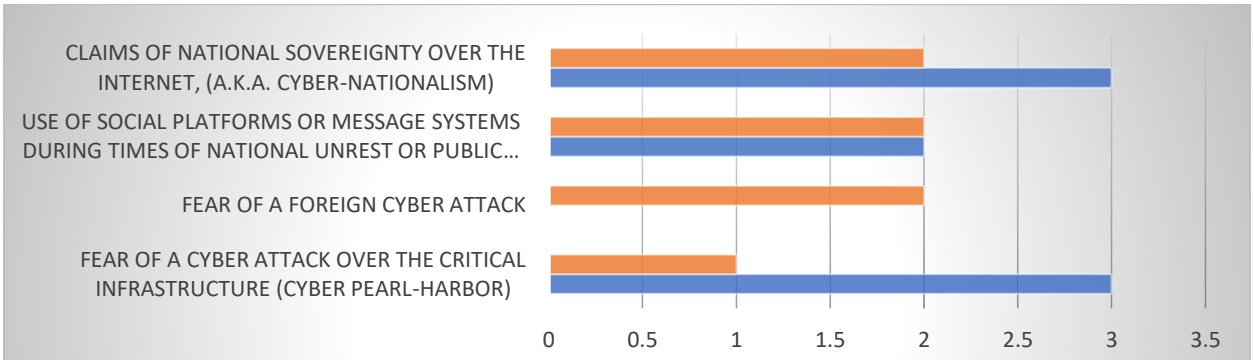
5.19.1. Political Factors

As mentioned in previous chapters, political factors are important because they address the type of government leadership, decisions and debate that may affect individuals and organizations within a nation-state in a specific period (PESTLE, 2015a, 2015b).

I identified political factors that are constantly manifested in the public debate and context and are part of the national security policies in the cases under study.

Figure 24 (see below) shows a representation of the different political factors that may prompt hybrid and democratic regimes to shut down the Internet. The "Y' axis contains the different political factors this dissertation identified, while the "X" axis contains the numbers of nation-states (democracies and hybrids) under study that used this element in their speech. In this way we could compare the similarities among different regimes.

Figure 24.- Comparison Between the Political Factors that Enable Democratic and Hybrid Regimes to Shut Down the Internet



	Fear of a Cyber Attack Over the Critical Infrastructure (Cyber Pearl-Harbor)	Fear of a Foreign Cyber Attack	Use of Social Platforms or Message Systems During Times of National Unrest or Public Protest	Claims of National Sovereignty over the Internet, (a.k.a. Cyber-Nationalism)
Hybrids	1	2	2	2
Democracies	3	0	2	3

Hybrid Regimes (2)	Venezuela and Russia
Democratic Regimes (3)	Australia, U.K., U.S.

The fear of a cyberattack over a critical infrastructure has been in the political debate since the attacks of September 2001 and they are the main concern in all cyber security policies created since those days. This is a common element between hybrid and democratic regimes. An important distinction between these regimes is the ownership and control over the critical infrastructure. While democratic regimes need (and call to create partnerships) the private sector in national security policies because they own and control the critical infrastructure, hybrid regimes circumstances are different. The critical infrastructure in Russia is mostly owned or controlled indirectly by the Russian government and it has been part of the national security strategy since 2000, during Vladimir Putin first presidential administration. The Russian approach is a top-down approach of controlling the entire Internet infrastructure; this is the reason for the creation of the so call "Blitzkrieg laws" over the Internet infrastructure that I mentioned in past chapters. Differently, democracies like the U.S. or the U.K. attempt to have the private sector as a partner, rather than as a subordinated.

The idea of a foreign attack is part of the hybrid regimes constant claims that they are the victims of foreign powers. This could be seen in the Russian scenario when, after the Snowden revelations of 2013, they made clear they were preparing for a foreign attack of the U.S. and its partners. Similarly, the Venezuelan government blamed foreign hackers of attacking the Twitter accounts of Nicolás Maduro and the ruling party and public sites (AVN/VTV, 2013; Belousov, 2014). While the process of trying to assert sovereignty over the Internet started after WSIS, the idea of fear of a foreign attack increased after the Snowden revelations.

A different scenario, shutting down the Internet because of the use of use of social network platforms or message systems during times of public protest, has been the subject of study when considering authoritarian regimes so much for academia like for civil society organizations. I

identified that hybrid regimes and well consolidated democracies have also similar concerns on this matter.

As referred many times, in 2011 during the London riots, Prime Minister Cameron blamed the Blackberry message system, Facebook and Twitter for allowing rioters to organize themselves and create chaos and disorder in London. As a result Cameron would call to shut down the entire Internet (Marsden, 2011; Nosowitz, 2011).

The U.S. also presents a case of trying to control, not only social networks, but also a message system. As this document explained before, all cellular service inside the Bay Area Rapid Transit (BART) got disrupted in San Francisco transit stations for three hours during a mass public protest and a year later, the DHS accepted some responsibility in the episode and referred to the SOP 303 emergency protocol (Brownlee, 2015; DeSoto, 2015).

In Venezuela the scenario is different. Censorship was common in Venezuela since Hugo Chavez was in power, however since 2013 local media has been under censorship and harassment over the foreign press became very common. The government started a campaign of repression to censor social networks platforms, specially twitter, and ended up with an Internet shutdown (Frank Bajak, 2014; Chao, 2014). Venezuelan authorities show a constant fear of a foreign attack they are not able to control. From their perspective, foreign criminals invaded social networks to attack accounts and manipulate information. At the same time, they also claimed that social networks, specially Twitter, are used by perpetrators of violence to create anguish in the population (Frak Bajak, 2014; noticias24, 2014). This last comment is a speech very similar to the British comments of “ill information” circulating within the social networks.

The Russian case came covered by a different political veil. Back in 2014, the Russian government enacted the so known as “bloggers law”. As I explained before, this new law

established that that any site with more than 3,000 visitors per day would be considered a media outlet and would be responsible for the accuracy of the information published. Because the law also implemented scanning software that allows the Russian government to review all content posted on the Internet, bloggers can no longer remain anonymous. As the law was passed, there was a common belief among experts and civil activists that the real targets were the social network platforms that originated abroad, like Facebook and Twitter (MacFarquhar, 2014; Zavyalova, 2014).

Finally, I will refer to the claims of national sovereignty over the Internet infrastructure and the flow of information, a tendency known as cyber nationalism. Despite of being so different between each other, constant claims of national sovereignty over the Internet are common characteristics of hybrid and democratic regimes. When it comes to the Internet, it is possible to find strong nationalisms subsisting even in different administrations within the same nation-state government. For consolidated democracies such as the U.S. and the U.K., claims of sovereignty over the Internet infrastructure are part of their national security policy. For the Australians, it means absolute competency of national authorities to regulate the Internet without foreign intervention. These claims became stronger since 2009 when the U.S. government declared the digital technology, the Internet included, a national asset.

For hybrid regimes claims of sovereignty over the Internet became a very important part of their politics after the Snowden revelations back in 2013, although they had nationalistic tendencies since early stages of the 21st century with the beginning of the administration of Hugo Chavez in Venezuela and Vladimir Putin in Russia. The Brazilian administration was the "standard-bearer" defending the cybernationalism when Dilma Rousseff (President at the time) recommended the increase of IXPs to keep the data flow within Brazilian territory. This put on the

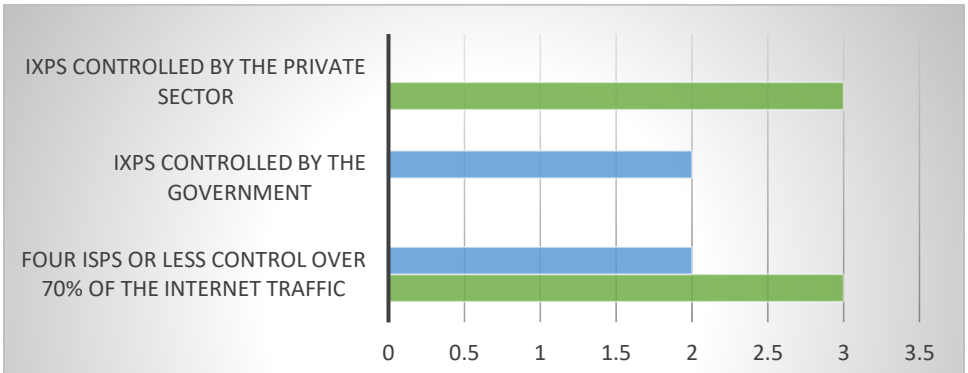
table governments' efforts not only to protect their data and their citizens, but also to subordinate the Internet infrastructure to national legislations (Costello, 2017; Keating, 2013b; Messmer, 2013). The clearest expression of cybernationalism is the production of the "Blitzkrieg laws" over the Internet infrastructure, the strongest effort of a government to keep the Internet completely under government control (Bodner, 2014). In a more colloquial but representative way, it is important to remember that Russian policymakers called to create a Patriotic Internet to fight against the west (Demirjian, 2015).

5.19.2. Technical Factors

Technical factors referred to the aspects a government may be able to manipulate and that can have access over industry and businesses. In this regard, technical factors define what organizations and individuals may be able to do in practical terms with the technology they have and the regulation in place (PESTLE, 2017). In the case of technical factors this dissertation identified two elements related to the state of the Internet infrastructure that are relevant to a policy like an Internet shutdown.

Figure 25 (see below) shows a representation of the technical political factors that may prompt hybrid and democratic regimes to shut down the Internet. The "Y' axe contains the different technical factors this dissertation identified, while the "X" axe contains the numbers of nation-states (democracies and hybrids) under study. In this way I could compare the similarities among different regimes.

Figure 25.- Comparison Between the Technical Factors that may enable Democratic and Hybrid Regimes to Shut Down the Internet



	Four ISPs or less control over 70% of the Internet traffic	IXPs controlled by the government	IXPs controlled by the private sector
Hybrid	2	2	0
Democracies	3	0	3

Hybrid Regimes (2)	Venezuela and Russia
Democratic Regimes (3)	Australia, U.K., U.S.

In this dissertation, I identified two technical factors that enable democratic and hybrid governments to shut down the Internet, ISPs and IXPs. These are the elements governments have tried to control to achieve an Internet shutdown within their own borders. Circumstances around these elements show coincidences and differences between hybrid and democratic regimes.

One of these elements is a coincidence between hybrid and democratic regimes: the existence of one ISP or few ISPs that handle over 70% of the Internet subscribers. This means, in both democratic and hybrid regimes, the Internet service is provided by a group of a few companies. In case of hybrid regimes those ISPs are mostly owned or controlled by the government and in the case of democratic regimes they are owned and controlled by the private sector. Despite their ownership, the reduced number of ISPs makes them vulnerable to governments' national security policies. As a matter of fact, this situation makes things even more critical because the

remaining ISPs that control between 10% and 30% of the Internet subscribers depend of the companies that control the other 70%.

As mentioned before, this scenario is distributed in this way: 1. In the case of Australia and Venezuela, one ISP handles around 90% of the Internet subscribers, 2. In the case of the U.S. and the U.K., fours ISPs control over 70% of the Internet subscribers, and 3. In the case of Russia, fours ISPs control over 70% of the Internet subscribers and the existent 13 ISPs (a very small number for a big territory as the Russian one with over 100'000,000 Internet subscribers) are under government control.

The second element is related to the control of the IXPs. Hybrid regimes may have none IXPs or few ones under control of the government or may have none. Democratic regimes tend to have multiple IXPs owned and managed by the private sector, and that hold multiple international connections.

The ownership and management of IXPs is also the only aspect where there are no similarities between hybrids and democracies when it comes to analyze the factors that may prompt those governments to shut down the Internet and is probably one of the most important conclusions this dissertation identified. The reason for this is that national government cannot control the international connections of complex IXPs designs.

IXPs are not ISPs. An IXP is a structure where Internet networks get together to peer or exchange traffic between their networks. IXPs don't sell Internet connectivity, but they improve it. Any network that wants to peer with other networks can connect to an IXP. In terms of management, different organizations may operate IXPs, either members who connect to the IXP or commercial organizations.

Most common customers of IXPs are ISPs. Some IXPs use more complex designs and therefore, they connect multiple networks using different protocols to carry the traffic. In this way, IXPs usually have multiple international connections. Having multiple IXPs privately owned with multiple Internet connections facilitates the Internet traffic to re-route, which means that even if a government tries to control an IXP, it cannot control it completely. This is the big difference between hybrid and democratic regimes; by having multiple IXPs privately-owned in their territories, the U.K., U.S. and Australia have a massive Internet infrastructure very difficult to control. This means shutting down the Internet is very unlikely.

Hybrid regimes are different. They lack of enough IXPs like Russia or have none like Venezuela. This makes the traffic very vulnerable if there is a need to re-route. Depending upon the level of government control, international connections may increase or no. This is the reason why in August 2017, the Russian government announced its plans to minimize the flow of Russian Internet traffic that runs through foreign-based IXPs. According to the Russian government, this plan intents that U.S. intelligence agencies don't get access to any sensitive data that runs through international connections. The new Russian bill proposes limiting foreign ownership over IXPs to 20%. This proposal follows the similar criteria of limiting Russian media holdings, a provision approved in 2014. If the bill is approved, it should get in force by July 2018 (Kantyshev & Sergina, 2017; The Moscow Times, 2017).

5.19.3. Legal Factors

Legal factors referred to laws and regulations that affect businesses and individuals in a specific nation-state. It is expected that legal statutes change time to time. This dissertation identified one legal factor common to all the cases under study, whether they are consolidated democracies or hybrid regimes: the existence of broad national security laws or telecommunication laws with unclear provisions about national security and the way governments should act.

National security laws are vague and unclear because they don't specify what the national interest is or the limits of the presidential authority to act when there is a national security threat. This ambiguity or lack of clarity is done on purpose, following the basic guidelines of what national security is. As I referred many times in this document, national security is a concept that refers to a set of policies created to protect the national interest and preserve the stability and survival of a nation-state (Bobbitt, 2002; Richards, 2012).

According to this logic, the national interest constantly changes as the geopolitical factors of a nation-state also change. In these circumstances, incumbent administrations create the set of national security policies after defining what the national interest is. Therefore, it is not strange that national security laws are broad and unclear because specific considerations or interpretations will be developed as the preferred geopolitical situations change and new enemies are created. Table 09 (see next page) provides an overview of the main laws cited by the nation-states under study.

Table 09.- Legal Provisions Used or Cited to Grant Powers to the Government Authorities to Shut Down the Internet

Nation-State	Legal Statute	Specific Provisions
Australia	Telecommunications Act of 1979 and amendments of 1997 and 2003	According to the provision 581 of the statute, the attorney general (after consultations with the Prime Minister and the Minister of Telecommunications) is entitled to request ISPs to stop providing Internet service under circumstances "prejudicial to security"
U.S.	Telecommunications Law of 1934 and amendments of 1996.	According to the representative of the U.S. government, control over the telecommunications is a prerogative of the president in fulfillment of the war powers of the telecom act (47 U.S. Code § 606). Such prerogative will be used according the specific case
U.K.	Communications Act of 2003	According to the section 132, OFCOM, the regulator, can request to any U.K.-based ISP the suspension of the service to preserve the "public order" or in case of a massive cyber-attack. OFCOM has the authority to act on behalf of the minister of culture, the one who has legal authority to "shut down the web"
U.K.	Civil Contingencies Act of 2004	Part 2 also would give to the executive branch legal authority to request to the ISPs the suspension of the Internet service. For this purpose, the executive branch is entitled to create emergency regulations if the U.K. faces a national security threat
Russia	The "Lugovoi Law" of 2014	It authorizes the prosecutor general to block access to media that disseminates calls for mass riots, extremist activities, or participation in unsanctioned mass public events. Limits to what should be blocked are not specified
Russia	First Anti-Terrorist Law of 2014	It stipulates that owners and operators of websites and services are required to store information at request of the government. They are obligated to store all information about the arrival, transmission, delivery, and processing of voice data, written text, images, sounds, or other kinds of action
Russia	Bloggers Law of 2014	It requires all web-based writers with posts that exceed 3000-page views to register with the government, as they are considered media outlets. The law also implements scanning software that allows the Russian government to review all content posted on the Internet

Russia	Law about Data Retention and Data Mining of 2014	The law requires foreign-Internet-companies to locate servers handling Russian Internet traffic inside the country and to store Russian users' data on these locally based servers for a minimum of six months
Venezuela	The Law of Social Responsibility and Quality of the Television in Venezuela of 2005	RESORTE forbids content considered "offensive," "violent," "disrupt public order," "disown pubic authorities," and "Induce homicide". It is the regulator the one to decide when the content falls into the previous categories. Actions to take may include shutting down the Internet

Despite any similarity, in the case of young democracies there is an element that is worth paying attention to even if young democracies are included in this study only with comparative purposes. Young democracies have specific legal and constitutional frameworks that refrain governments of shutting down the Internet. As I can remember the two young democracies under study, Brazil and Mexico, have specific provisions that protect the Internet: Brazil enacted the law known as "Marco Civil," which gives to the Internet legal protection and Mexico declared the Internet a human right and granted to it constitutional protection.

This is a characteristic that only can be appreciated within young democracies. Nevertheless, although they cannot shut down the Internet, this doesn't mean that they cannot apply other limitations over the Internet infrastructure.

6. Conclusions

In 2005, a small group of academics was involved in something known as OpenNet Initiative reported that the Internet had been shut down in Nepal, a small nation-state located in South Asia (OpenNet Initiative, 2005). At the time, the king of Nepal, King Gyanendra, declared a "state of emergency" in Nepal and shut down all communications means, including the Internet. However, because the number of Internet users in Nepal was less than 1% of habitants, the entire world barely noticed what happened. The situation was dramatically different in 2011 when the Egyptian Internet shutdown occurred. Egyptian Internet users counted for over 30% of its population, and Egypt had a more sophisticated Internet infrastructure than Nepal. After this event, the world questioned the importance of having the Internet in times of national unrest. Since those days, there have been multiple publications (academic and non-academic) about the actions of authoritarian regimes to control the Internet during times when there are protests against them. As a result, members of the academic sectors and activists credited the Internet of being a catalyzer for democratic change.

For some time, this extreme form of government control, baptized as an Internet shutdown, Internet kill switch or Internet blackout, was assumed to exist or to be considered only by authoritarian regimes. I concluded in this dissertation that this is not the case. In this project, I proposed to look at other regimes (not the authoritarian ones), the well-consolidated democracies and hybrid regimes. Therefore, I drafted the following research questions that guided this dissertation:

RQ1: What is the global scope of the Internet shut down phenomenon?

RQ2: What justifications do democratic and hybrid regimes use to shut down or to consider shutting down the Internet?

RQ3: What are the political, legal and technical factors that enable a government to shut down the Internet?

To answer these research questions, this project combined two areas of research: law and social sciences. The purpose of this combination is using social sciences theories and methodologies to analyze legal documents, political and security speeches related to the action of shutting down the Internet, and news and articles to contribute greater objectivity and accuracy to legal opinions.

The next paragraphs will develop the mains conclusions of this dissertation.

Despite any justification, hybrid and democratic regimes have considered an Internet shutdown, they executed one or claimed an accident. In both types of regimes, they believed that legal or political debate was worth to discuss the issue. Regarding the kind of regime, governments never discarded this extreme form of government control over the Internet and, this one remains as part of the mindset of all government authorities of the nation-states under study.

By framing different concepts of national security within different speeches, hybrid and democratic regimes try to justify the inclusion of an Internet shutdown within their national legislation. When authorities deliver a speech, the securitization theory (theoretical framework for this dissertation) points to the importance of the "referent object," within the terms of that speech. I identified the referent object with the national interest, that thing that needs to be protected to preserve the survival and stability of a nation-state.

This dissertation has concluded that hybrid and democratic regimes have different referent objects in mind: the critical infrastructure, the public order and national data (from governments and citizens). However, there are areas of overlapping. In this scenario, there are several conclusions to draw:

1. Hybrid regimes are concerned about the critical infrastructure like the well-consolidated democracies are,
2. Well-consolidated democracies are as concern about the internal public order and the use of social network platforms to disrupt it, as hybrid regimes are,
3. Hybrid regimes are particularly concerned about the flow of data and the idea that all attacks that may affect them are "foreign" ones

The achievement of these conclusions comes after the analysis of government representative speeches following the securitization theory of the Copenhagen School, alongside with legal, political and technical indicators specific to the nation-states selected as case studies.

As a result, it is possible to see that even when is about technical, legal and political factors that enable a government to shut down the Internet, there are strong similarities between hybrid and democratic regimes.

Concerning audiences to address, when considering the national security policy of any regime, the private sector is a pivotal partner to analyze. In well-consolidated democracies, the private sector is the owner of the Internet infrastructure and the critical infrastructure. In hybrid regimes, the private sector is the one responsible for the data flow in and out of the territory of those regimes. In both cases, the private sector can reach and maintain networks governments cannot. It is the presence of the private sector and the multiple international connections the private sector allows, what makes the difference whether actions to shut down the Internet can or cannot be successful.

About this situation, it is important to remember that, in all cases, under study, the Internet service is concentrated in a few companies, ISPs that handle between the 70% and 90% of the Internet subscribers. As concluded, this is not only a similar element but also one that needs

attention. Although it is true that the private sector controls ISPs in well-consolidated democracies and, in the case of hybrid regimes they are under government control (even if the government does not own them), it is not in their ownership where the danger is. The risk of having so few ISPs in control of the Internet service is because then the Internet itself becomes more vulnerable to government control, whether this occurs in extraordinary circumstances or because the government tries indeed to control the Internet. In other words, no matter the type of regime, it is easier to manage a few ISPs because those few companies handle over the 70% of the Internet subscribers.

As this research pointed out before, although hybrid regimes have created a set of laws to control every aspect of the Internet, democratic regimes have demonstrated that they don't trust in their ISPs either. This lack of trust was the case during the debate of some control policies the Australian government wanted to impose and during the Internet kill switch debate in the U.S.

Given these governments' concerns, the current scenario shows this panorama:

Table 10.- ISPs that control between 70%-90% of Internet Subscribers in Hybrid and Democratic Regimes

Nation-State	Companies	Percentage of the market they control
Australia	Telstra	It controls around the 90% of the market of the Internet service
U.S.	Comcast, Charter, AT&T, and Verizon	They control around 76% of the market of the Internet service
U.K.	BT, TalkTalk, Virgin Media, and Sky	They control around the 90% of the market of the Internet service
Russia	Known as the "Big Four": MTS, VimpelCom, MegaFon, and Tele2	They control around 90% of the market of the Internet service
Venezuela	CANTV	It controls over 90% of the market of the Internet service

The situation is even more critical because the ISPs that control the remaining traffic depend on the ones that control most of the traffic for their proper functionality.

6.1. Reasons to Not Shut Down the Internet

It was not one of the goals of this dissertation identifying the reasons why hybrid and democratic regimes did not shut down or did not considered doing so. However, during the analysis of the case studies selected for this project, I could identify the factors to keep the Internet on (to not shut it down). Such factors can be appreciated in the specific circumstances of the Internet infrastructure that surround the case studies I used for comparison purposes.

In the case of the democratic regimes, the evidence comes from Mexico concretely. When it comes to political factors, Mexico has a significant public debate to increase the Internet connectivity and improve its quality and speed, more than in any of the other cases under study. This situation is critical in Mexico for the lack of IXPs and the very few ISPs that nation-state has. This combination has Mexico in a an awkward position: (1) Mexico is the nation-state with one of the slowest Internet speed in North America and (2) has the last place among the 35 members of the OECD (Castanares, 2017).

Additionally, among political factors, Mexican authorities have used the Internet to facilitate the protection of self-defense forces and fight against drug dealing activities. Drug dealing is one of the most dangerous illegal operations in Mexico, and the government has not been able to create successful policies to fight against it.

From a legal point of view, Mexico and Brazil, young democracies under study, have both included in their national legislation provisions to protect the Internet. These provisions don't

forbid actions that affect the Internet, such as acts of censorship. However, any new regulation to shut down the Internet would be an unconstitutional or illegal one.

Finally, from a technical point of view, the evidence comes from a hybrid regime, Turkey. Turkey is one of the few nation-states that had poisoned the DNS. Poisoning the DNS slows down or prevents the access to web pages and services. Most likely mail and remote file systems may be inaccessible. This disruptive activity implies that any external communication is at risk when the DNS does not work correctly. By poisoning the DNS, governments are using a disruptive technique to tackle specific sources of information they don't want their citizens to have access. However, what makes this technique more pervasive than censorship actions is the perception for Internet users that nothing is wrong. As I pointed out before, DNS cache poisoning diverts the Internet traffic away from legitimate servers towards fake ones. In this regard, not only prevents to Internet users to access what they want but also it is dangerous because it can spread from DNS server to DNS server. The Turkish experience and evidence tell us that the government of that nation-state prefers to use more disruptive techniques of Internet instead of the Internet kill switch. It is possible to hypothesize that tools to control the Internet, other than the kill switch, serve better to the government's goals.

6.2. Limitations

This section will describe a specific set of constraints and vulnerabilities this project had to address.

1. Internet shutdowns started in 2005, and they continue until the moment this project was created. Although RQ1 discusses the global scope of the problem, it is possible that by

the time of submitting this dissertation, there are more cases of Internet shutdowns than the ones initially reported.

2. At the time of presenting the dissertation proposal for this project, young democracies remained aside of the consideration or the use of Internet shutdowns as control policies. For this reason, I did not include them as comparative cases studies. However, in 2016, the government of one young democracy (India) shut down the Internet in several cities and created an administrative regulation to allow the government of that nation-state to shut down the Internet under specific circumstances. Despite this episode, I preserved the original research design and, young democracies remained as case studies of nation-states that did not shut down the Internet and never considered doing it.
3. This study proposed a multiple case study. This project had as a proposition that by comparing cases of similar regimes, it was expected to identify related factors that surround the shutdown of the Internet, for hybrids and well-consolidated democracies. However, this study did not find clear distinctions between both types of regimes. On the contrary, this study identified common elements rather than distinguish differences among the factors that enable hybrid and democratic regimes to shut down the Internet.
4. Regarding the language barriers these clarifications are required:

   I did not need any assistance to search and analyze text in English, Spanish and Portuguese. In the Turkish and Russian cases, it was necessary to recruit help for the translation of sources in their respective language from software, friends and fellow students fluent in those languages.

6.3. Directions for Future Study

This study was an exploratory research project about the Internet shutdowns in well-established democracies and hybrid regimes. Research findings followed the order of the research questions:

1. The global scope of the Internet shut down phenomena,
2. Main elements of the securitizing speech that government agents use to justify an Internet shutdown,
3. Political, legal and technical factors that enable a democratic or hybrid government to shut down the Internet.

These findings extend the current literature about Internet shutdowns that has devoted to studying mostly authoritarian regimes. However, I believe future research needs to analyze a few issues this dissertation identified:

1. Young democracies are also considering shutting down the Internet and at least one young democracy, India, has done it. Therefore, more research is needed to determine if these regimes include new legal, political, and technical factors that enable a government to shut down the Internet (different from the ones established for hybrids and well-established democracies). About authoritarian regimes, updated research is also necessary as they continue applying this extreme policy over the Internet and recently they are using different reasons not related to national security (f/e avoid cheating in school examinations).
2. This study concluded in the middle of what is considered a re-born of the nation-states as main entities of international law and the election of nationalist governments. These

two elements are considered part of a new order where government actors present the globalization process present as a “failure” and nation-states retake the control over the telecommunications systems and therefore, from the Internet infrastructure (Grygiel, 2016; Mazower, 2014). It is possible to anticipate that this “new order” will bring new policies of “cybernationalism” which may include the possibility of shutting down the Internet. This new context and its policies require attention for the future.

3. This project was limited to analyze Internet shutdowns at a national level only. In the future, studies need to be conducted to examine the same extreme policy from different points of view, such as a) the response of the international legal system to Internet shutdowns, b) the response of the Internet community (represented by ICANN) and c) Internet shutdowns as a tool of cyberwarfare.
4. Trying to control the Internet within the borders of a nation-state implies, to some extent, that governments also try to control resources beyond their territory, especially for the multiple connections the Internet can create. Although the governments' practice of trying to extend their sovereignty is not new, the new element, in this case, is the Internet, and this is a whole further aspect to study. Moreover, this is an element that needs more discussion after the creation of non-binding agreements to use already existent international law frameworks over the Internet infrastructure, such as the law of the sea and space law.

6.4. Lessons from this Study and Why the Conclusions are Important

The possibility of shutting down the Internet implies a higher level of government control, especially from the Executive branch or a new government body created with that purpose. In this regard, Internet shutdowns are opposed to two essential aspects related to the Internet itself: 1) the multi stakeholder model and 2) the open architectural design of the Internet.

These two elements, a form of governance and a characteristic of the Internet, keep the latter without a single point of control. They both succeeded, to some extent, during the ICANN transition that operated in 2016. However, this model faces challenges of those nation-states that advocate for a government-based-model to regulate the Internet or that pretend to have independent Internets. Among those nation-states, it is possible to find governments that considered the Internet shut down as an acceptable policy within their legal systems. Among those governments, there are also well-consolidated democracies.

Despite the type of government, it is important to remember that no matter what nation-state executes an Internet shutdown, there is always an impact over the international Internet traffic, especially, for neighbor nation-states. This potential consequence is one of the reasons why Internet shutdowns have consequences at a global level. Multiple national economies and human rights could be altered in more than one nation-state.

In Latin America, there is an old phrase that says, “When the United States sneezes, Latin America gets pneumonia”. This phrase refers to the effects specific problems or policy decisions the U.S. may go through and how they affect its neighbor nation-states in the south. Parallels scenarios exist in the rest of the world. This situation also has unpredictable consequences that may revert to the U.S. when the economies of Latin America find themselves affected by policy decision taken by that government.

As the last statement for this project, it is essential to make a point related to the policymakers who can to decide if an Internet shutdown must be executed or included in their national legislation. As far as this research could identify, and just to point an example, no study is conclusive as what could happen with the critical infrastructure after an Internet shutdown takes place. On this subject, it is essential that policy makers remember that, according to what they want to accomplish, their job is not curing the disease by killing the patient but curing the disease to save the patient.

All case-studies in this project pointed out that shutting down the Internet is a remedy to prevent different diseases, such as attacks over the critical infrastructure, attacks over the communication means of the ruling party and attempts to destabilize what governments consider the internal public order. However, no evidence supports the fact that shutting down the Internet is a remedy to all these "diseases." On the contrary, and from an economic perspective, previous studies account for the negative effects of Internet shutdowns on the GDP (GNI, 2018; Rydzak, 2017). From a technical perspective, varying opinions refer that isolating or disconnecting individual sectors, like electrical utilities and telecommunications lines from the Internet, is a technique to protect the critical infrastructure (Knapp, 2011).

Finally, I will refer to what this disruptive policy of shutting down the Internet may bring for the future. As mentioned before, the disconnection of the local Internet brings consequences over the international Internet traffic. How much? It depends of the nation-state that suffers the disconnection. When it comes to the freedom of expression, or what some people call the digital speech, I would like to use a quote from Professor Balkin from the Information Society Project at Yale (ISP) (Balkin, 2018, p.1153):

> "The digital speech flows through an elaborated privately-owned infrastructure of communication. Today our practical ability to speak is subject to the decisions of private infrastructure owners, who govern the digital spaces in which people communicate with each other."

If we depend on the decision of private corporations, what would happen when the decisions of these private corporations are constraint by unclear national security policies?

And finally, shutting down the Internet (as analyzed so far) implies the concentration of power in one government authority: the one who decides that the Internet should be shut down. We live in a time of a reborn of the concept of nation-states as the main actors of international law and the only sources of laws and public governance. What are the implications of a disruptive policy, such as shutting down the Internet, in this new international scenario over the multi stakeholder model and the open architecture design of the Internet? The latter one guarantees that there is no a single point of control for the Internet and the first one is a governance model that involves multiple stakeholders when it comes to the decision making about the Internet infrastructure.

When trying to foresee the future, the Internet community must consider three elements and the implications over an open and free Internet, as we have become to know.

7. Appendixes

The following chapters contain all the documents previously mentioned during the development of this dissertation as part of the appendixes.

7.1. Appendix 1: U.S. Constitution, Article II

Section 1.

The executive power shall be vested in a President of the United States of America. He shall hold his office during the term of four years, and, together with the Vice President, chosen for the same term, be elected, as follows:

Each state shall appoint, in such manner as the Legislature thereof may direct, a number of electors, equal to the whole number of Senators and Representatives to which the State may be entitled in the Congress: but no Senator or Representative, or person holding an office of trust or profit under the United States, shall be appointed an elector.

The electors shall meet in their respective states, and vote by ballot for two persons, of whom one at least shall not be an inhabitant of the same state with themselves. And they shall make a list of all the persons voted for, and of the number of votes for each; which list they shall sign and certify, and transmit sealed to the seat of the government of the United States, directed to the President of the Senate. The President of the Senate shall, in the presence of the Senate and House of Representatives, open all the certificates, and the votes shall then be counted. The person having the greatest number of votes shall be the President, if such number be a majority of the whole number of electors appointed; and if there be more than one who have such majority, and have an equal number of votes, then the House of Representatives shall immediately choose by ballot one of them for President; and if no person have a majority, then from the five highest on the list the said House shall in like manner choose the President. But in choosing the President, the votes shall be taken by States, the representation from each state having one vote; A quorum for this purpose shall consist of a member or members from two thirds of the states, and a majority of all the states shall be necessary to a choice. In every case, after the choice of the President, the person having the greatest number of votes of the electors shall be the Vice President. But if there should remain two or more who have equal votes, the Senate shall choose from them by ballot the Vice President.

The Congress may determine the time of choosing the electors, and the day on which they shall give their votes; which day shall be the same throughout the United States.

No person except a natural born citizen, or a citizen of the United States, at the time of the adoption of this Constitution, shall be eligible to the office of President; neither shall any person be eligible to that office who shall not have attained to the age of thirty five years, and been fourteen Years a resident within the United States.

In case of the removal of the President from office, or of his death, resignation, or inability to discharge the powers and duties of the said office, the same shall devolve on the Vice President,

and the Congress may by law provide for the case of removal, death, resignation or inability, both of the President and Vice President, declaring what officer shall then act as President, and such officer shall act accordingly, until the disability be removed, or a President shall be elected.

The President shall, at stated times, receive for his services, a compensation, which shall neither be increased nor diminished during the period for which he shall have been elected, and he shall not receive within that period any other emolument from the United States, or any of them.

Before he enter on the execution of his office, he shall take the following oath or affirmation:--"I do solemnly swear (or affirm) that I will faithfully execute the office of President of the United States, and will to the best of my ability, preserve, protect and defend the Constitution of the United States."

Section 2.

The President shall be commander in chief of the Army and Navy of the United States, and of the militia of the several states, when called into the actual service of the United States; he may require the opinion, in writing, of the principal officer in each of the executive departments, upon any subject relating to the duties of their respective offices, and he shall have power to grant reprieves and pardons for offenses against the United States, except in cases of impeachment.

He shall have power, by and with the advice and consent of the Senate, to make treaties, provided two thirds of the Senators present concur; and he shall nominate, and by and with the advice and consent of the Senate, shall appoint ambassadors, other public ministers and consuls, judges of the Supreme Court, and all other officers of the United States, whose appointments are not herein otherwise provided for, and which shall be established by law: but the Congress may by law vest the appointment of such inferior officers, as they think proper, in the President alone, in the courts of law, or in the heads of departments.

The President shall have power to fill up all vacancies that may happen during the recess of the Senate, by granting commissions which shall expire at the end of their next session.

Section 3.

He shall from time to time give to the Congress information of the state of the union, and recommend to their consideration such measures as he shall judge necessary and expedient; he may, on extraordinary occasions, convene both Houses, or either of them, and in case of disagreement between them, with respect to the time of adjournment, he may adjourn them to such time as he shall think proper; he shall receive ambassadors and other public ministers; he shall take care that the laws be faithfully executed, and shall commission all the officers of the United States.

Section 4.

The President, Vice President and all civil officers of the United States, shall be removed from office on impeachment for, and conviction of, treason, bribery, or other high crimes and misdemeanors.

7.2. Appendix 2: U.K. Communications Act 2003, Section 132

An Act to confer functions on the Office of Communications; to make provision about the regulation of the provision of electronic communications networks and services and of the use of the electro-magnetic spectrum; to make provision about the regulation of broadcasting and of the provision of television and radio services; to make provision about mergers involving newspaper and other media enterprises and, in that connection, to amend the Enterprise Act 2002; and for connected purposes.

132.- Powers to require suspension or restriction of a provider's entitlement

(1) If the Secretary of State has reasonable grounds for believing that it is necessary to do so—

(a) to protect the public from any threat to public safety or public health, or

(b) in the interests of national security, he may, by a direction to OFCOM, require them to give a direction under subsection (3) to a person ("the relevant provider") who provides an electronic communications network or electronic communications service or who makes associated facilities available.

(2) OFCOM must comply with a requirement of the Secretary of State under subsection (1) by giving to the relevant provider such direction under subsection (3) as they consider necessary for the purpose of complying with the Secretary of State's direction.

(3) A direction under this section is—

(a) a direction that the entitlement of the relevant provider to provide electronic communications networks or electronic communications services, or to make associated facilities available, is suspended (either generally or in relation to particular networks, services or facilities); or

(b) a direction that that entitlement is restricted in the respects set out in the direction.

(4) A direction under subsection (3)—

(a) must specify the networks, services and facilities to which it relates; and

(b) except so far as it otherwise provides, takes effect for an indefinite period beginning with the time at which it is notified to the person to whom it is given.

(5) A direction under subsection (3)—

(a) in providing for the effect of a suspension or restriction to be postponed, may provide for it to take effect only at a time determined by or in accordance with the terms of the direction; and

(b) in connection with the suspension or restriction contained in the direction or with the postponement of its effect, may impose such conditions on the relevant provider as appear to OFCOM to be appropriate for the purpose of protecting that provider's customers.

(6) Those conditions may include a condition requiring the making of payments—

(a) by way of compensation for loss or damage suffered by the relevant provider's customers as a result of the direction; or

(b) in respect of annoyance, inconvenience or anxiety to which they have been put in consequence of the direction.

(7) Where OFCOM give a direction under subsection (3), they shall, as soon as practicable after doing so, provide that person with an opportunity of—

(a) making representations about the effect of the direction; and

(b) proposing steps for remedying the situation.

(8) If OFCOM consider it appropriate to do so (whether in consequence of any representations or proposals made to them under subsection (3) or otherwise), they may, without revoking it, at any time modify the terms of a direction under subsection (3) in such manner as they consider appropriate.

(9) If the Secretary of State considers it appropriate to do so, he may, by a direction to OFCOM, require them to revoke a direction under subsection (3).

(10) Where OFCOM modify or revoke a direction they have given under subsection (3), they may do so—

(a) with effect from such time as they may direct;

(b) subject to compliance with such requirements as they may specify; and

(c)to such extent and in relation to such networks, services or facilities, or parts of a network, service or facility, as they may determine.

(11) It shall be the duty of OFCOM to comply with—

(a) a requirement under subsection (9) to revoke a direction; and

(b) a requirement contained in that direction as to how they should exercise their powers under subsection (10) in the case of the required revocation.

7.3.Critical Infrastructure: A Comparative Approach

Table 11.- Critical Infrastructure: Comparative Definitions and Sectors Involved				
	U.S.	**European Commission**	**Australia**	**Brazil**
Definition	According to the USA Patriot Act of 2001 ((42 U.S.C. 5195c(e)), the critical infrastructure refers to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Klemm & Johnson, 2010; U.S. Congress, 2001)	According to the Document COM (2004) 702 final, the critical infrastructure is defined as "physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services" (European Commission, p.3, 2004)	According to the Australian Government book of Cybersecurity Strategy of 2009, the critical infrastructure "are the systems which, if rendered unavailable or otherwise compromised, could result in significant impacts on Australia's economic prosperity, international competitiveness, public safety, social wellbeing or national defense and security. The identification of systems of national interest is not a static process and a flexible approach is required to enable the Australian government to respond to the changing environment–in terms of technology, usage, threat and risk. It is for this reason that the identification of systems of national interest must be informed by an ongoing assessment of	According to the Brazilian Green Book of Cyber-security, the critical infrastructure is related to "installations, services, goods and systems that if destroyed, it would have a serious, social, economic, politics, environmental, international over the national security and the society" (as cited by (Almeida Advogados, p.8, 2015)

			risk" (Australian Government, p.12, 2009) According to the Attorney General, critical infrastructure can be defined as "physical facilities, supply chains, information technologies and communications networks which, if destroyed, degraded or rendered unavailable for an extended period, would adversely impact on the social or economic well-being of the nation or affect Australia's ability to ensure national security" (Wilson, p.702, 2014)	
Sectors involved	According to the Presidential Policy Directive from 2013 (PPD-21), sectors involved within the critical infrastructure classification are: 1. Chemical 2. Commercial Facilities 3. Communications 4. Critical Manufacturing	According to the document # COM (2004) 702 final from the European Commission titled "Critical Infrastructure Protection in the fight against terrorism," critical infrastructure includes: 1. Energy installations and networks Communications and Information Technology 2. Finance 3. Health Care	According to the Australian Government book of Cybersecurity Strategy of 2009, critical infrastructure includes: 1. Electricity grids, 2. Water storage and distribution, Aviation and maritime transport, Telecommunications networks 3. Systems of high economic value that support	According to the Brazilian Green Book of Cyber-security, critical infrastructure includes: 1. Energy 2. Transportation 3. Water supply 4. Telecommunications 5. Finance 6. Information (Almeida Advogados, 2015)

	5. Dams 6. Defense Industrial Base 7. Emergency Services 8. Energy 9. Financial Services 10. Food and Agriculture 11. Government Facilities 12. Healthcare and Public Health 13. Information Technology 14. Nuclear Reactors, Materials, and Waste 15. Transportation Systems 16. Water and Wastewater Systems (DHS, 2013)	4. Food 5. Water 6. Transport 7. Production, storage and transport of dangerous goods 8. Government (European Commission, 2004)	electronic transactions and hold sensitive intellectual property and commercial data associated with major international trade negotiations (Australian Government, 2009b)	

7.4. IRB Forms

IRB#: _____
DATE REC'D
(For IRB Use Only)

SYRACUSE UNIVERSITY
Institutional Review Board

APPLICATION FOR DESIGNATION AS RESEARCH EXEMPT FROM IRB REVIEW

Initial review generally requires 5-7 business days from the date an exempt application is received by the IRB Office. Should modifications and/or clarifications be requested by the IRB, additional review time may be required.

On average the IRB advises it may take 4 weeks for the IRB exempt review process. (This includes the investigators response time.)

***NOTE*: The Principal Investigator (PI) must be a person who holds a faculty appointment or other administrative position of Director or higher. If you have any questions regarding this IRB requirement call the IRB office at 315.443.3013 for guidance.**

Principal Investigator/Faculty Member Information

First Name: Jennifer	Middle Initial:	Last Name: Stromer-Galley
Position: Associate Professor		
Department: School of Information Studies	College:	
Campus Address: 220 Hinds Hall		
Campus Phone : (315) 443-1823		Fax :
Email: jstromer@syr.edu		Cell Phone (optional):

Student/Research Staff Information ☐NA

First Name: Patricia	Last Name: Vargas-Leon	
☒ Graduate Student ☐ Undergraduate Student ☐ Other:		
Department: School of Information Studies	College:	
Local/Campus Address: 337 Hinds Hall		
Local/Campus Phone: (315) 443 - 5509		Fax:
Email: pavargas@syr.edu		Cell Phone (optional):

TITLE OF PROPOSAL: Addressing the ultimate form of cybersecurity control: a multiple case-study for the "Iinternet Kill Switch"

NOTE: Collaborative Institutional Training Initiative (CITI) is ***not*** required for research determined to be exempt. CITI is required for researchers involved in expedited or full board studies.

1A. IS IT RESEARCH?

The definition of research as defined by the Department of Health and Human Services (DHHS) regulations: "Research means a ***systematic investigation***, including research development, testing and evaluation, designed to develop or contribute to ***generalizable knowledge.***" 45 CFR 46.102 (d)

To be considered a "systematic investigation", the concept of a research project must:

- Attempt to answer research questions (in some research, this would be a hypothesis).
- Be methodologically driven, that is, it collects data or information in an organized and consistent way.
- Analyze data or information in some way, be it quantitative or qualitative data.
- Draw conclusions from the results.

A. Is your project a systematic investigation? ☒ Yes ☐ No

B. Provide an explanation for your response: Drawing from the securitization theory of the Copenhagen School, this project attempts to identify the causes why democracies and hybrid regimes shut down or considered shutting down the Internet claiming reasons of national security. The final outcome of the research is a contribution to the study of information policies, specifically from the Internet. Causes to analyze include legal, political and economical reasons.

"Generalizable knowledge" would include one or more of the following concepts:

- The knowledge contributes to a theoretical framework of an established body of knowledge.
- The primary beneficiaries of the research are other researchers, scholars and practitioners in the field of study.
- Publication, presentation or other distribution of the results is intended to inform the field of study.
- The results are expected to be generalized to a larger population beyond the site of data collection.
- The results are intended to be replicated in other settings.
- Web based publication for professional purposes.

C. Will your project contribute to generalizable knowledge? ☒ Yes ☐ No

D. Provide an explanation for your response: This research project attempts to contribute to the studies of the Internet governance, an interdisciplinary area that includes professionals and researchers from areas such as information science, law, politics, communications, economics and engineering. The theory to be applied, the Securitization theory of the Copenhagen School, has been previously used to analyze an aspect called "the militarization of the Internet," but there are no studies regarding governments' control of the Internet infrastructure, which is the main purpose of the current project.

*If "yes" to question A. **AND** C above the activity is considered research. Continue completing the application.*

1B. IS IT HUMAN SUBJECTS RESEARCH?

A. Is the data that is being obtained about living individuals? ☒ Yes ☐ No

B. Are data collected through interaction or intervention with individuals (e.g., interviews, surveys, or any direct contact)? ☐ Yes ☒ No

C. Is identifiable individual private information being obtained (e.g., chart reviews, information from data or tissue repositories)? ☐ Yes ☒ No

D. Are data or specimens received by the investigator with identifiable private information? ☐ Yes ☒ No

E. Are the data/specimens coded with a link back to the individual? ☐ Yes ☒ No

*If "yes" to question A. above **AND** "yes" to one or more questions from B-E in section 1B, the activity is considered human research. Continue completing the application.*

Protocols that do not meet the criteria for *research **AND** human subjects research* need not be submitted to the IRB for review or for a determination that the project falls into an exempt category.

Additional guidance for publically available data:
Some research involves the analysis of data about humans for which the regulatory definition of "human subject" is not met. One example is research that involves only the analysis of de-identified data contained within publicly available datasets (available to any one regardless of occupation, purpose, or affiliation, and those individuals who are responsible for posting the dataset had legitimate access to the data and have employed the necessary mechanisms to ensure the privacy and confidentiality of the individuals about whom the data were collected).

While the activity described above meets the regulatory definition of research, the definition of human subject is not met because data about a living person is not obtained through interaction or intervention, and no private, identifiable information about a living individual is obtained.

2. CATEGORIES FOR EXEMPTION

I/We certify that the above research project involves human subjects only in one or more of the following categories, and will be carried out using standard methods. Please check the number next to category(ies) pertinent to the research.[1]

☐ **1.** Research conducted in established or commonly accepted educational settings, involving normal educational practices, such as:
   (a) research on regular and special education instructional strategies, or
   (b) research on the effectiveness of or the comparison among instructional techniques, curricula, or classroom management methods, and
   (c) the research must not involve prisoners as participants

☐ **2.** Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior unless:
   (a) information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and
   (b) any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.
   (c) If the research involves children, the procedures must be limited to educational tests and observation of public behavior where the investigators do not participate in the activities being observed.
   (d) The research must not involve prisoners as participants.

☐ **3.** Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior that is not exempt under paragraph (2) of this section, if:
   (a) the human subjects are elected or appointed public officials or candidates for public office; or
   (b) federal statute(s) require(s) without exception that the confidentiality of the personally identifiable information will be maintained throughout the research and thereafter.
   (c) The research must not involve prisoners as participants.

☒ **4.** Research involving the collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens, if these sources are publicly available or if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects. [Note: *To qualify for this exemption ALL of the data, documents, records, or specimens must be in existence **before** the project begins.]*
   (a) The research must not involve prisoners as participants.

---

[1] *The Federal Regulations also include a sixth category for exempt research, the Institutional Review Board has the discretion to determine what categories to recognize and does not recognize research under category 6 as qualifying for exemption. If you have questions, please contact the IRB at 315.443.3013 or orip@syr.edu.*

6. Taste and food quality evaluation and consumer acceptance studies a) if wholesome foods without additives are consumed or (b) if food is consumed that contains a food ingredient at or below the level and for a use found to be safe, or agricultural chemical or environmental contaminant at or below the level found to be safe by the Food and Drug Administration or approved by the Environment Protection Agency or the Food Safety and Inspection Service of the U.S. Department of Agriculture.

☐ **5.** Research and demonstration projects which are conducted by or subject to the approval of department or agency heads, and which are designed to study, evaluate, or otherwise examine:
(a) public benefit or service programs;
(b) procedures of obtaining benefits or services under those programs;
(c) possible changes in or alternatives to those programs or procedures; or
(d) possible changes in methods or levels of payment for benefits or services under those programs.
(e) The protocol must be conducted pursuant to specific federal statutory authority.
(f) The protocol must have no statutory requirements for IRB review.
(g) The protocol must not involve significant physical invasions or intrusions upon the privacy interests of the participants.
(h) The protocol must have authorization or concurrence by the funding agency.
(i) The research must not involve prisoners as participants.

3. SCREENING QUESTIONS

A. Does any part of the research require that subjects be deceived?	☐Yes	☒ No
B. Will research expose human subjects to discomfort or harassment beyond levels encountered in daily life?	☐Yes	☒ No
C. Could disclosure of the subjects' responses outside the research reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation?	☐Yes	☒ No
D. Will individuals involuntarily confined or detained in penal institutions be subjects of the study?	☐Yes	☒ No
E. For research proposed under category 2, will research involve surveys, interview procedures, or observation of public behavior with children where the researcher will interact with the children?	☐Yes	☒ No
F. For research proposed under category 4, will any of the data, documents, records, pathological specimens, or diagnostic specimens be collected or come into existence after the date you apply for exemption?	☐Yes	☒ No
G. For research proposed under category 4, will any of the information obtained from data, documents, records, pathological specimens, or diagnostic specimens that come from private sources be recorded by the investigator in such a manner that subjects can be identified directly or through identifiers linked to the subjects?	☐Yes	☒ No

*If you checked **YES** to **ANY** of the questions above, your research is **NOT EXEMPT.** Do not complete this application. Submit an **application for Expedited or Full Board Review**.*
*If you have checked **NO** to **ALL** of the questions above, your research may be exempt. Please complete the remainder of the exempt application.*

4. RATIONALE FOR EXEMPTION

Please briefly describe the proposed research and explain in clear language why you believe this research should be exempted from IRB review.

The purpose of this investigation is to understand the extent, conditions and factor that can lead to government closing off access to the Internet, among democratic and hybrid regimes. Those conditions will be deduced by looking at a variety of texts and videos available in the Internet; the data includes from news reports to speeches of government actors. All this data is publicly available and there is no interaction with any participant at any level, there are no interviews, no observations and no surveys. Any reference to political speech comes from Internet newspapers, magazines, blogs that do not require any special permission and are available to any Internet user. There is no data from particular sources that need a special permission to be accessed.

5. RECRUITMENT

Please submit all recruitment materials including but not limited to: recruitment flyers, e-mails, letters and/or scripts.

Describe plans for recruitment and how contact will be made:
No recruitment will be required

Will you be contacting participants through a contact list or list server provided by a department, organization, company or school? If yes, provide a letter of support from the individual authorized to provide you with this information. More than one letter may be required.
☒ Does not apply
☐ Letter(s) attached
Comments:

Will you require support from the University for selection or contact information of participants? If the answer is yes, you will be required to obtain a letter of cooperation from the Office of Institutional Research and Assessment (OIRA).
☒ Does not apply
☐ Letter attached

Will this research be conducted in a school or is it funded by the US Department of Education?
☒ No. **(Skip to Section 6)**
☐ Yes. If yes, complete the form found at:
http://orip.syr.edu/files/Research%20Sponsored%20by%20the%20US%20Department%20of%20Education%20and-or%20Conducted%20in%20Schools.doc

6. METHODS

All research measures which will be used during this study including sample questions, questionnaires, recruitment scripts, etc. must be included with the application.

Provide a detailed description of what participants will be required to do.

There are no participants in this study

Will this research be conducted by SU investigators in foreign countries?
☒ No.
☐ Yes. If yes, an additional form related to international research must be completed and submitted with this application: International Research Appendix.

7. INFORMED CONSENT REQUIREMENT

*(This is **not** required for Category 4)*

Please provide a copy of the written or electronic informed consent document or oral consent script you will use in your study. Please note this document must include the following minimum required elements:

1. A statement that clearly explains that the study is research. The purpose of the research should be described in lay language, avoiding the use of technical terms and using language appropriate to the targeted subject group.
2. A statement that describes what procedures will be followed, clearly explaining what participation in the study will involve.

3. It must be clear that participation is voluntary and participants can withdraw from the study at any time without penalty.
4. Contact information for the investigator.
5. For adult participants, a statement that the subject is 18 years or older must appear as part of the consent.
6. For internet research add the following statement:
   Whenever one works with email or the internet there is always the risk of compromising privacy, confidentiality, and/or anonymity. Your confidentiality will be maintained to the degree permitted by the technology being used. It is important for you to understand that no guarantees can be made regarding the interception of data sent via the internet by third parties.

8. SIGNATURES

This is to acknowledge that I take full responsibility for the conduct of the research. **Investigators of studies exempt from IRB review are responsible for the ethical conduct of research and obtaining informed consent when appropriate.** (If this study is being conducted by a student, a faculty member must sign in the space provided). Electronic and /or faxed signatures are acceptable.

Signed: _____ Date: 12/7/15
(Faculty member)

Name (printed): Jennifer Stromer Galley

Signed: _____ Date: 12/07/2015
(Student, if applicable)

Name (printed): Patricia A. Vargas-Lein

Graduate ☒ Undergraduate ☐

All notifications will be sent via email. Hard copies will be only be provided upon request.

RETURN ONE COPY OF THE COMPLETED APPLICATION TO:

SYRACUSE UNIVERSITY
INSTITUTIONAL REVIEW BOARD
Office of Research Integrity and Protections
121 Bowne Hall
Syracuse, New York, 13244-1200
Phone: 443-3013
Fax: 443-9889
orip@syr.edu

7.5.IRB Approval

SYRACUSE UNIVERSITY
Institutional Review Board
MEMORANDUM

TO: Jennifer Stromer-Galley
DATE: December 18, 2015
SUBJECT: **Determination of Exemption from Regulations**
IRB #: 15-349
TITLE: *Addressing the Ultimate Form of Cybersecurity Control: A Multiple Case-Study for the Internet Kill Switch*

The above referenced application, submitted for consideration as exempt from federal regulations as defined in 45 C.F.R. 46, has been evaluated by the Institutional Review Board (IRB) for the following:

1. determination that it falls within the one or more of the five exempt categories allowed by the organization;
2. determination that the research meets the organization's ethical standards.

It has been determined by the IRB this protocol qualifies for exemption and has been assigned to category **4**. This authorization will remain active for a period of five years from **December 16, 2015** until **December 15, 2020**.

CHANGES TO PROTOCOL: Proposed changes to this protocol during the period for which IRB authorization has already been given, cannot be initiated without additional IRB review. If there is a change in your research, you should notify the IRB immediately to determine whether your research protocol continues to qualify for exemption or if submission of an expedited or full board IRB protocol is required. Information about the University's human participants protection program can be found at: http://orip.syr.edu/human-research/human-research-irb.html Protocol changes are requested on an amendment application available on the IRB web site; please reference your IRB number and attach any documents that are being amended.

STUDY COMPLETION: Study completion is when all research activities are complete or when a study is closed to enrollment and only data analysis remains on data that have been de-identified. A Study Closure Form should be completed and submitted to the IRB for review (Study Closure Form).

Thank you for your cooperation in our shared efforts to assure that the rights and welfare of people participating in research are protected.

Tracy Cromp, M.S.W.
Director

DEPT: Information Studies, 220 Hinds Hall **STUDENT:** Patricia Vargas-Leon

Office of Research Integrity and Protections
121 Bowne Hall Syracuse, New York 13244-1200
(Phone) 315.443.3013 ♦ (Fax) 315.443.9889
orip@syr.edu ♦ www.orip.syr.edu

Bibliography

Abouzeid, R. (2011). Tunisia: How Mohammed Bouazizi Sparked a Revolution -. Retrieved March 10, 2014, from TIME website: http://content.time.com/time/magazine/article/0,9171,2044723,00.html

accessnow. (2017). #KeepItOn. Retrieved March 21, 2017, from accessnow website: https://www.accessnow.org/keepiton/

Ackerman, J. M. (2016). Mexico Is Not a Functioning Democracy. Retrieved February 27, 2016, from Foreign Policy website: http://foreignpolicy.com/2016/02/23/obama-pena-nieto-mexico-corruption/

AFP. (2014). Vladimir Putin seeks power to "unplug" Russia from Internet: Report - The Economic Times. *The Economic Times*. Retrieved from http://economictimes.indiatimes.com/news/international/business/vladimir-putin-seeks-power-to-unplug-russia-from-internet-report/articleshow/42895647.cms

AIS Marine Traffic. (2017). Vessel details for: YANTAR (SAR) - MMSI 273546520, Call Sign RMM91 Registered in Russia. Retrieved December 28, 2017, from AIS Marine Traffic website: http://www.marinetraffic.com/en/ais/details/ships/shipid:1215053/mmsi:273546520/vessel:YANTAR

Alexander, M. (2008). Democratization and Hybrid Regimes: Comparative Evidence from Southeast Europe. *East European Politics & Societies*, *22*(4), 928–954. Retrieved from http://eep.sagepub.com.libezproxy2.syr.edu/content/22/4/928

Almeida Advogados. (2015). Segurança Cibernética no Brasil. Retrieved February 25, 2016, from Almeida Advogados website: http://www.almeidalaw.com.br/download/2015 05 06 Cybersecurity v5 %282%29.pdf?utm_source=Mondaq&utm_medium=syndication&utm_campaign=inter-article-link

Anderson, L. (2011). Demystifying the Arab Spring : Parsing the Differences Between Tunisia, Egypt, and Libya. *Foreign Affairs Foreign Affairs*.

Andrews, L. (2012). *I know who you are and I saw what you did : social networks and the death of privacy* (1st Free P). Retrieved from http://www.worldcat.org/title/i-know-who-you-are-and-i-saw-what-you-did-social-networks-and-the-death-of-privacy/oclc/709673179&referer=brief_results

Ang, P. (2012). Shutting down the mobile phone and the downfall of Nepalese society, economy and politics. *Pacific Affairs*, *85*(3), 547–561.

Angarita, Y. (2017). Conatel prepara reglamento para actuar sobre las redes sociales. Retrieved July 3, 2017, from El Universal website: http://www.eluniversal.com/noticias/politica/conatel-prepara-reglamento-para-actuar-sobre-las-redes-sociales_655275

Ángeles, V. (2013). Aprueban reformas en materia de telecomunicaciones [Telecommunication Amendments approved]. Retrieved October 2, 2015, from http://diarioelreloj.com.mx/index.php/local-articulos/8838-aprueban-reformas-en-materia-de-telecomunicaciones

Aquino, S. (2009). Should Obama Control the Internet? Retrieved August 23, 2017, from Mother Jones website: http://www.motherjones.com/politics/2009/04/should-obama-control-

internet/

Arnaudo, D., Alva, A., Wood, P., & Whittington, J. (2013). Political And Economic Implications of Authoritarian Control of the Internet. In J. Butts & S. Shenoi (Eds.), *7th Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection (ICCIP)*. Retrieved from http://apps.webofknowledge.com.libezproxy2.syr.edu/full_record.do?product=WOS&search_mode=GeneralSearch&qid=1&SID=3D2Vs43bCS1SeGHKHt3&page=3&doc=30

Arreola, F. (2014). Qué logro de la Reforma en Telecomunicaciones de EPN: Slim vende y abre totalmente la competencia. Retrieved October 2, 2015, from SDP Noticias website: http://www.sdpnoticias.com/columnas/2014/07/08/que-logro-de-la-reforma-en-telecomunicaciones-de-epn-slim-vende-y-abre-totalmente-la-competencia

Arsu, S. (2011). Turkey Protests New Internet Filters. Retrieved April 21, 2014, from The New York Times website: http://www.nytimes.com/2011/05/16/world/europe/16turkey.html?_r=0

Asamblea Nacional de la Republica Bolivariana de Venezuela. *Ley de Responsabilidad Social en Radio, Television y Medios Electronicos*. , (2004).

Asmolov, G. (2015). Welcoming the Dragon: The Role of Public Opinion in Russian Internet Regulation. *Center for Global Communication Studies, Internet Policy Observatory*. Retrieved from http://www.global.asc.upenn.edu/publications/welcoming-the-dragon-the-role-of-public-opinion-in-russian-internet-regulation/

Asseburg, M. (ed). (2012). SWP Research Paper - Protest, Revolt and Regime Change in the Arab World. Retrieved August 16, 2012, from http://www.swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP06_ass.pdf

Astakhov, P. (2016). "Russia can be disconnected from the global Internet": Klimenko in an interview with RT. Retrieved September 20, 2017, from RT in Russian website: https://russian.rt.com/russia/article/346157-intervyu-klimenko-internet#.WGUFPJOgxig.twitter

Auer, M. R. (2011). The Policy Sciences of Social Media. *Policy Studies Journal*, *39*(4), 709–736. https://doi.org/10.1111/j.1541-0072.2011.00428.x

Australian Government. (2009a). *Cyber Security Strategy*. Retrieved from https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG Cyber Security Strategy - for website.pdf

Australian Government. (2009b). Cyber Security Strategy. Retrieved February 23, 2016, from Commonwealth of Australia website: https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG Cyber Security Strategy - for website.pdf

AVN/VTV. (2013). Vicepresidente Arreaza: datos electorales están totalmente protegidos [Vice president Arreaza: electoral data is totally protected]. Retrieved September 28, 2015, from Venezolana de Televisión website: http://www.vtv.gob.ve/articulos/2013/04/14/vicepresidente-arreaza-datos-electorales-estan-totalmente-protegidos-4490.html

AVN. (2014). Restituyen servicio Aba en Táchira tras hechos violentos. Retrieved August 17, 2017, from AVN website: http://www.avn.info.ve/node/223024

Azpura, A., Guerra, C., & Rivas, J. L. (2019). Phishing by Venezuelan government puts activists and Internet users at risk.

Babbie, E. (2017). The Basics of Social Research. Retrieved April 30, 2017, from Thomson

website: https://books.google.com/books?id=1_lSEh6AAfYC&printsec=frontcover&source=gbs_book_other_versions#v=onepage&q&f=false

Bailey, C. (2007). *A guide to qualitative field research* (2nd ed.). Retrieved from http://www.worldcat.org/title/guide-to-qualitative-field-research/oclc/65165341&referer=brief_results

Bajak, F. (2014). Venezuela Cuts Off Internet, Blocks Communication For Protestors. Retrieved September 22, 2014, from LatinoVoices website: http://www.huffingtonpost.com/2014/02/21/venezuela-internet-_n_4832505.html

Bajak, F. (2014, February 22). Venezolanos Libran otra Batalla para Acceder a la Información [Venezuelans Fighitng a Battle for Information Access]. *La Republica Peru*. Retrieved from http://larepublica.pe/22-02-2014/venezolanos-libran-otra-batalla-para-acceder-a-la-informacion

Bajak, F., & Sequera, V. (2014). Internet a crucial Venezuela battleground. Retrieved July 18, 2017, from U.S. News website: https://www.usnews.com/news/world/articles/2014/02/21/internet-a-crucial-venezuela-battleground

Balkin, J. M. (2018). Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. *Davis University of California Law Review*, *51*, 1149–1210. Retrieved from https://lawreview.law.ucdavis.edu/issues/51/3/Essays/51-3_Balkin.pdf

Bambauer, D. E. (2011). Conundrum. *Minnesota Law Review*, *96*, 584. Retrieved from http://papers.ssrn.com/abstract=1807076

Barbara, V. (2013, September 26). Have a Nice Day, N.S.A. *The New York Times*. Retrieved from http://www.nytimes.com/2013/09/27/opinion/have-a-nice-day-nsa.html

Barber, S. A., & Fleming, J. E. (2011). Constitutional Theory, the Unitary Executive and the Rule of Law. *American Society for Political and Legal Philosophy*, *50*, 156–166.

Barboza Gutiérrez, O. (2012). El 7 de Octubre (October 7th). Retrieved March 16, 2017, from Un Nuevo Tiempo website: http://partidounnuevotiempo.org/inicio/index.php/articulos-de-opinion/333-omar-barboza-gutierrez-el-7-de-octubre

Barboza Gutiérrez, O. (2014). Un CNE imparcial [An impartial CNE]. Retrieved March 16, 2017, from UN Nuevo Tiempo website: http://www.partidounnuevotiempo.org/inicio/index.php/articulos-de-opinion/1884-un-cne-imparcial

Barilleaux, R. J., & Maxwell, J. (2017). Has Barack Obama Embraced the Unitary Executive? *PS: Political Science & Politics*, *50*(01), 31–34. https://doi.org/10.1017/S1049096516002055

Barnard-Wills, D., & Ashenden, D. (2012). Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture*, *15*(2), 110–123.

Barnard, A., & Mackey, R. (2012, November 29). Internet Shutdown Reported Across Syria. *The New York Times*. Retrieved from http://thelede.blogs.nytimes.com/2012/11/29/internet-outage-reported-across-syria/

BART. (2011). Statement on temporary wireless service interruption in select BART stations on Aug. 11. Retrieved February 16, 2016, from BART Bay Area Rapid Transit website: http://www.bart.gov/news/articles/2011/news20110812

Barth, R. (1997). International regulation of encryption : technology will drive policy. *Borders in Cyberspace : Information Policy and the Global Information Infrastructure Borders in Cyberspace Ed. by Brian Kahin and Charles Nesson*.

Baxter, P., & Jack, S. (2008). *The Qualitative Report Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers*. *13*(2), 12–1. Retrieved from http://nsuworks.nova.edu/tqr

BBC. (2016). Ukraine crisis: What's going on in Crimea? Retrieved March 17, 2018, from BBC News website: http://www.bbc.com/news/world-europe-25182823

BBC. (2017). Venezuela chief prosecutor to probe election fraud claim. Retrieved November 29, 2017, from BBC News website: http://www.bbc.com/news/world-latin-america-40812312

BBC Mundo. (2017). Al menos diez muertes marcan el día de las cruciales y polémicas elecciones en Venezuela para elegir una Asamblea Constituyente [At Least Ten Deaths Mark the Day of the Crucial and Controversial Elections in Venezuela to Elect a Constituent Assembly]. Retrieved March 12, 2018, from BBC Mundo website: http://www.bbc.com/mundo/noticias-america-latina-40768241

Beal, V. (2010). The Differences Between the Internet and the Web. Retrieved March 10, 2017, from Webopedia website: http://www.webopedia.com/DidYouKnow/Internet/Web_vs_Internet.asp

Becerra, R. (2008). *Internet Llega a la Constitution [Internet and its Inclusion in the Constitution]*. Retrieved from https://archivos.juridicas.unam.mx/www/bjv/libros/6/2540/7.pdf

Beijnum, I. van. (2011). How Egypt did (and your government could) shut down the Internet. *Ars Technica Law & Disorder/Civilization & Discontents*. Retrieved from http://www.bgp4.as/internet-exchanges

Bell, M. (2011, August 12). BART San Francisco cut cell services to avert protest. *Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/worldviews/post/bart-san-francisco-cut-cell-services-to-avert-protest/2011/08/12/gIQAfLCgBJ_blog.html

Belousov, V. (2014). 'Unpredictable West' could isolate Russian internet, Putin's aide warns. Retrieved March 23, 2015, from RT Question More website: http://rt.com/politics/196848-russia-internet-west-plan/

Belson, D. (2016). National Internet Outages - The New Normal? Retrieved July 31, 2017, from The Akamai Blog website: https://blogs.akamai.com/2016/09/national-internet-outages-the-new-normal.html

Benadava, S. (1982). *Derecho internacional público [Public International Law]* (2a ed. act). Retrieved from http://www.worldcat.org/title/derecho-internacional-publico/oclc/10231726&referer=brief_results

Benbasat, I., Goldstein, D., & Mead, M. (1987). The case research strategy in studies of information systems. Retrieved March 17, 2014, from MIS Quarterly website: http://www.jstor.org/stable/248684

Bernard, D. (2015). Russia Possibly Testing Internet Kill Switch. Retrieved January 28, 2016, from Voice of America website: http://www.voanews.com/content/russia-possibly-testing-internet-kill-switch/3020489.html

Bhalla, R. (2009). Turkey and Russia on the Rise. Retrieved April 21, 2014, from Stratfor website: http://www.stratfor.com/weekly/20090317_turkey_and_russia_rise

Billington, J. (2016). Gabon government shuts down internet for four days following election uproar. Retrieved September 5, 2016, from International Business Times website: http://www.ibtimes.co.uk/gabon-shuts-down-internet-four-days-biggest-nationwide-blackout-ever-1579773

Blair, T. (2010). Documentation Required. Retrieved March 27, 2017, from Daily Telegraph website: http://www.dailytelegraph.com.au/blogs/tim-blair/documentation-required/news-

story/75dbd6cbe50b4c40d99dedf6bc5be301
Blockmon, R. (2018). What is an Internet Service Provider (ISP)? Retrieved February 27, 2018, from Study.com website: https://study.com/academy/lesson/what-is-an-internet-service-provider-isp-definition-examples-quiz.html
Boas, T. (2006). Web: the control of Internet Use in Non Democratic Regimes. In J. Zysman & A. Newman (Eds.), *How revolutionary was the digital revolution? National Responses, Market Transitions, and Global Technology*. California: Standford Business Books.
Bobbitt, P. (2002). *The Shield of Achilles: War, Peace, and the Course of History*. Knopf.
Bodkin, H. (2017). NHS cyber attack spreads worldwide. Retrieved May 12, 2017, from The Telegraph website: http://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/
Bodner, M. (2014, September 19). Russians' Internet Increasingly Subject to Control. *The Moscow Times*. Retrieved from https://themoscowtimes.com/articles/russians-internet-increasingly-subject-to-control-39603
Bowman, W., & Camp, J. (2013). Protecting the internet from dictators: Technical and policy solutions to ensure online freedoms. *Innovation Journal*, *18*(1).
Bracci Roa, L. (2013). *Jorge Arreaza: suspensión momentánea de Internet se hizo para proteger de hackers a web del CNE [Jorge Arreaza: momentary suspension of the Internet was done to protect the CNE web from hackers]*. Retrieved from https://www.youtube.com/watch?v=kn1vmbvxoIs
Braman, S. (2006). *Change of state : information, policy, and power*. Cambridge Mass.: MIT Press.
Braman, S. (2010). Internet Policy. In M. Consalvo & C. Ess (Eds.), *The Handbook of Internet Studies* (pp. 137–167). Wiley-Blackwell.
Briscoe, N. (2000). Understanding The OSI 7-Layer Model. Retrieved March 20, 2019, from PC Network Advisor website: https://www.os3.nl/_media/2014-2015/info/5_osi_model.pdf
Brodkin, J. (2016). Comcast and Charter may soon control 70% of 25Mbps Internet subscriptions. Retrieved November 12, 2018, from arstechnica website: https://arstechnica.com/information-technology/2016/01/comcast-and-charter-may-soon-control-70-of-25mbps-internet-subscriptions/
Brodzinsky, S. (2015). Venezuela opposition leader Leopoldo López jailed for nearly 14 years. Retrieved March 6, 2017, from theguardian website: https://www.theguardian.com/world/2015/sep/11/venezuela-opposition-leader-leopoldo-lopez-sentenced-to-14-years-in-jail
Brownlee, L. (2015). U.S. Supreme Court Asked To Review Secrecy Of DHS's Wireless Kill Switch Policy. Retrieved September 15, 2015, from In Homeland Security website: http://inhomelandsecurity.com/u-s-supreme-court-asked-to-review-secrecy-of-dhss-wireless-kill-switch-policy/
Brownlie, I. (2003). *Principles of public international law* (6th ed.). Oxford ;New York: Oxford University Press.
Brownlie, I. (2012). *Brownlie's Principles of Public International Law* (8th ed.; S. P. Crawford, Ed.). Oxford; New York.
BT. (2017). BT, Sky, TalkTalk and Virgin Media join together to protect children online - BT. Retrieved February 4, 2018, from BT website: http://home.bt.com/tech-gadgets/tech-news/bt-sky-talktalk-and-virgin-media-join-together-to-protect-children-online-11364220067801

Burke, S. (2017). The first Twitter president: Hugo Chávez. Retrieved September 17, 2017, from CNN Tech website: http://money.cnn.com/2017/01/26/technology/hugo-chavez-first-twitter-president-venezuela-trump/index.html

Butler, A. (2007). Security and the "Smokeless War". A Critical Look at "Security as Speech Act" Theory via Internet Security in China. *Op On Politicis*, *2*(2). Retrieved from https://journals.uvic.ca/index.php/onpolitics/issue/view/70

Buzan, B. (1998). *Security : a new framework for analysis*. Boulder Colo.: Lynne Rienner Pub.

Cabinet Office. (2011). *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

cadsvm. (2010). *Chávez: Hay que actuar contra Noticiero Digital (y Globovisión)*. Retrieved from https://www.youtube.com/watch?v=3f0kCyUZhHI

Calabresi, S. G., & Yoo, C. S. (2003). The Unitary Executive During the Second Half of the Century. Retrieved October 5, 2018, from Harvard Journal of Law and Public Policy website: https://search-proquest-com.libezproxy2.syr.edu/docview/235205819?pq-origsite=summon&accountid=14214

Calabresi, S. G., & Yoo, C. S. (2008). *The unitary executive : presidential power from Washington to Bush*. Retrieved from https://books.google.com/books?id=4sJhrLROSc8C&pg=PA4&lpg=PA4&dq="all+of+our+nation's+presidents+have+believed+in+the+theory+of+the+unitary+executive."&source=bl&ots=2HzDfT57AP&sig=KyDz-gvdNojaCdIYNGubGZuSIqc&hl=en&sa=X&ved=2ahUKEwiBseCZ1ZjeAhVhneAKHafRAa

Calabresi, S., & Yoo, C. (1997). The Unitary Executive During the First Half-Century. *Faculty Scholarship at Penn Law*, 1450–1561. Retrieved from https://scholarship.law.upenn.edu/faculty_scholarship/718

Cameron, D. (British P. (2011a). PM statement on disorder in England. Retrieved March 16, 2017, from Speeches - GOV.UK website: https://www.gov.uk/government/news/pm-statement-on-disorder-in-england

Cameron, D. (British P. (2011b, August 11). UK riots: text of David Cameron's address to Commons. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/news/uknews/crime/8695272/UK-riots-text-of-David-Camerons-address-to-Commons.html

Campbell, K. (2009). *The rhetorical act thinking, speaking and writing critically*. Belmont Calif.: Wadsworth Pub. Co.

Cannon, C., Jordan, J., Keller, R., & Feeney, T. (2005). *Committee on the Judiciary Subcommittee on Commercial and Administrative Law*. Retrieved from https://www.gpo.gov/fdsys/pkg/CHRG-110hhrg42214/pdf/CHRG-110hhrg42214.pdf

Carpes, G. (2012). Brazil seeks to prevent "internet blackout" during World Cup. Retrieved September 2, 2015, from Terra website: http://esportes.terra.com.br/futebol/copa-2014/brasil-se-prepara-para-evitar-apagao-de-internet-durante-copa,8c221d81c499a310VgnCLD200000bbcceb0aRCRD.html

Carpizo, J. (2007). Concepto de democracia y sistema de gobierno en América Latina. *Boletín Mexicano de Derecho Comparado*, *XL*(119), 325–348. Retrieved from http://www.redalyc.org/resumen.oa?id=42711903

Carstensen, S. (2014). Google Online Security Blog: Google's Public DNS intercepted in Turkey. Retrieved December 15, 2016, from Google Blog website: https://security.googleblog.com/2014/03/googles-public-dns-intercepted-in-turkey.html

Casilli, A. A., & Tubaro, P. (2011). Why Net Censorship in Times of Political Unrest Results in More Violent Uprisings: A Social Simulation Experiment on the UK Riots. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1909467

Castanares, I. (2017). Internet en México es cara y lenta [Internet in Mexico is Expensive and Slow]. Retrieved March 30, 2018, from El Financiero website: http://www.e-consulta.com/medios-externos/2017-05-08/internet-en-mexico-es-cara-y-lenta

CCG-NLU. (2016). 11 Indian States have Shutdown the Internet 37 times since 2015. Retrieved October 3, 2016, from Legally India website: http://www.legallyindia.com/blogs/11-indian-states-have-shutdown-the-internet-37-times-since-2015

CDT. (2009). Analysis of S. 773, Cybersecurity Act of 2009. In *Center for Democracy & Technology*. Retrieved from https://www.cdt.org/security/20090511_rocksnowe_analysis.pdf

CEPAL. (2016). Cepal: Venezuela tiene la velocidad de Internet mas lenta de Latinoamerica [Cepal: Venezuela has the slowest Internet from Latin America]. Retrieved March 20, 2017, from CEPAL website: http://www.el-nacional.com/noticias/historico/cepal-venezuela-tiene-velocidad-internet-mas-lenta-latinoamerica_7514

CEPROMAT. (2014). Brazil starts preventive action against "internet blackout" during the 2014 World Cup. Retrieved September 3, 2015, from CEPROMAT website: http://jao.cepromat.mt.gov.br/~hom-cepromat/index.php/mnu-noticias/353-brasil-inicia-processo-preventivo-contra-apagao-de-internet-durante-copa-de-2014

CGI.br. (n.d.). About the CGI.br. Retrieved August 18, 2017, from CGI.br - website: https://cgi.br/about/

Chalfant, M. (2017). Trump pressed to secure US critical infrastructure. Retrieved February 5, 2018, from The Hill website: http://thehill.com/policy/cybersecurity/326218-trump-pressed-to-secure-us-critical-infrastructure

Chang, A. (2013). Why Undersea Internet Cables Are More Vulnerable Than You Think | WIRED. Retrieved April 20, 2015, from WIRED website: http://www.wired.com/2013/04/how-vulnerable-are-undersea-internet-cables/

Chang, S.-I., Wu, H.-C., & Cho, H.-C. (2011). The Development of Digital Divide Assessment Mechanism for SMEs: A Perspective from the Taiwan Manufacturing Industry. *Journal of Global Information Technology Management*, *14*(1), 6–34.

Chao, L. (2014). Twitter, Other Apps Disrupted in Venezuela Amid Protests of Maduro Government. Retrieved February 22, 2014, from The Wall Street Journal website: http://online.wsj.com/news/articles/SB10001424052702303775504579397430033153284

Cheng, J., & Nam, I.-S. (2014, December 27). North Korea Blames U.S. for Internet Shutdown. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/pyongyang-blames-u-s-for-norths-internet-outage-1419656909

Chester, R. (2016). Telstra suffers new network outage. Retrieved March 19, 2017, from news.com.au website: http://www.news.com.au/technology/telstra-nbn-and-adsl-customers-hit-by-new-network-outage/news-story/4e221a5b1e9ae3193e4a7422d026cae2

Chinea, E., & Daniel, F. J. (2010). Venezuela's Chavez calls for internet controls. Retrieved March 6, 2016, from Reuters website: http://www.reuters.com/article/us-venezuela-chavez-idUSTRE62D05I20100314

CircleID. (2016). Notorious Russian Ship Yanter Suspected of Cutting Syria's Undersea Internet Cables. Retrieved July 28, 2017, from CircleID - Internet infrastructure website: http://www.circleid.com/posts/20161014_notorious_russian_ship_yanter_suspected_syrian_cable_cut/

Civic Impulse. (2017). Details for S. 773 (111th): Cybersecurity Act of 2010. Retrieved August 13, 2017, from GovTrack.us website: https://www.govtrack.us/congress/bills/111/s773/details

Clabough, R. (2015). DHS Ordered to Explain Secret Plan to Shut Down Phone Service. Retrieved September 15, 2015, from NewAmerican website: http://www.thenewamerican.com/usnews/item/20645-dhs-ordered-to-explain-secret-plan-to-shut-down-phone-service

Clark, D., Berson, T., & Lin, H. S. (2014). *At the Nexus of Cybersecurity and Public Policy* (D. Clark, T. Berson, & H. S. Lin, Eds.). https://doi.org/10.17226/18749

Clavio, G. (2008). *Uses and Gratifications of Internet Collegiate Sport Message Board Users*. ProQuest.

Clegg, N. (MP). (2011). Deputy Prime Minister's speech on the Arab Spring. Retrieved September 11, 2015, from Speeches - GOV.UK website: https://www.gov.uk/government/speeches/deputy-prime-ministers-speech-on-the-arab-spring

CNN. (2010). *CNN transcripts. State of the Union with Candy Crowley. Interviews With Senators Lieberman, Murkowski, Feinstein and Lugar*. Retrieved from http://transcripts.cnn.com/TRANSCRIPTS/1006/20/sotu.01.html

Cole, W. M. (2011). Individuals v. states: The correlates of Human Rights Committee rulings, 1979-2007. *Social Science Research*, *40*(3), 985–1000. https://doi.org/10.1016/j.ssresearch.2010.10.003

Comision de Atencion a Grupos Vulnerables. (2014). Senado de la República. Retrieved September 15, 2015, from Diario de los Debates. Senado de la Republica de los Estados Unidos Mexicanos - LXIII Legislatura website: http://www.senado.gob.mx/index.php?ver=sp&mn=3&sm=2&lg=&ano=&id=44921

Comunello, F. (2012). Will the revolution be tweeted? A conceptual framework for understanding the social media and the Arab Spring. *Islam and Christian-Muslim Relations*, *23*(4), 453–470.

Conversation, T. (2013, March 6). National economy grows but some non-mining states in recession. *The Conversation*. Retrieved from http://theconversation.com/national-economy-grows-but-some-non-mining-states-in-recession-12670

Costello, J. (2017). Cyber nationalism and the new world order. Retrieved May 2, 2017, from GCN website: https://gcn.com/articles/2017/03/20/cyber-nationalism.aspx

Côté, A. (2016). Agents without agency: Assessing the role of the audience in securitization theory. *Security Dialogue*, *47*(6), 541–558. https://doi.org/10.1177/0967010616672150

Coughlin, A. (2015). Dyn Launches Internet Alerts for Unprecedented Visibility Into Fundamental Internet Performance Issues. Retrieved November 3, 2017, from Dyn website: http://dyn.com/blog/dyn-launches-internet-alerts-for-unprecedented-visibility-into-fundamental-internet-performance-issues/

Cousin, G. (2005). Case Study Research. *Journal of Geography in Higher Education*, *29*(3), 421–427. https://doi.org/10.1080/03098260500290967

Cowie, J. (2011a). Egypt Leaves the Internet. Retrieved from renesys website:

http://www.renesys.com/2011/01/egypt-leaves-the-internet/
Cowie, J. (2011b). Watching Algeria. Retrieved June 22, 2016, from Dyn Research website: http://research.dyn.com/2011/02/watching-algeria/
Cowie, J. (2014). Internet kill switch - Renesys. Retrieved March 11, 2014, from renesys website: http://www.renesys.com/?s=Internet+kill+switch&x=0&y=0
Cowie, J. (2015). Brazil's Winning Internet: Diversity of Infrastructure Gives It a Leg Up. Retrieved September 1, 2015, from WIRED website: http://insights.wired.com/profiles/blogs/brazil-s-winning-internet#axzz3kWPv5nHY
CPNI. (2017). Critical National Infrastructure. Retrieved March 13, 2017, from Centre for the Protection of National Infrastructure website: https://www.cpni.gov.uk/critical-national-infrastructure-0
Crawford, A. (2009). UK-email law "attack on rights." Retrieved February 4, 2018, from BBC News website: http://news.bbc.co.uk/2/hi/uk_news/7819230.stm
Crawford, J. (2013). *Brownlie's Principles of Public International Law*. Oxford University Press.
Creswell, J. (2003). *Research design : qualitative, quantitative, and mixed method approaches* (2nd ed.). Retrieved from http://www.worldcat.org/title/research-design-qualitative-quantitative-and-mixed-method-approaches/oclc/49558924&referer=brief_results
Creswell, J. W. (2013). *Qualitative inquiry and research design: choosing among five approaches*. SAGE Publications.
Crook, J. R. (2010). Secretary of State Addresses Human Rights and the Internet . *The American Journal of International Law*, *104*(2), 291–294. Retrieved from http://search.proquest.com.libezproxy2.syr.edu/docview/577318129?accountid=14214
D'Orazio, D. (2014). Crimeans are now using the Russian internet -. Retrieved September 17, 2017, from The Verge website: https://www.theverge.com/2014/8/2/5962145/crimeans-are-now-using-the-russian-internet
Dahl, R. (2005). Democratic Polities in Advances Countries: Success And Challenge. *New Worldwide Hegemony. Alternatives for Change and Social Movements*, 51–70. Retrieved from http://bibliotecavirtual.clacso.org.ar/ar/libros/hegeing/Dahl.pdf
Danckert, S. (2016, May 22). Telstra hit with another outage. *The Sydney Morning Herald*. Retrieved from http://www.smh.com.au/business/consumer-affairs/telstra-hit-with-another-outage-20160522-gp0uj0.html
DarkvanM. (2009). Jay Rockefeller: Internet should have never existed. Retrieved August 10, 2017, from YouTube Video website: https://www.youtube.com/watch?v=Ct9xzXUQLuY
David, G. (2016). Donald Trump Wants Bill Gates To Turn Off The Internet To Stop ISIS. Retrieved from International Business Times website: http://www.ibtimes.com/donald-trump-wants-bill-gates-turn-internet-stop-isis-2215683?utm_source=RevContent&utm_medium=Right2&utm_term=Internal&utm_campaign=Recommended
DCM. (2015). Internet Exchange Points. Retrieved November 10, 2015, from Data Center Map website: http://www.datacentermap.com/ixps.html
Deahl, D. (2017). Russia bans anonymous web surfing tools. Retrieved July 31, 2017, from The Verge website: https://www.theverge.com/2017/7/31/16070934/russia-ban-proxies-vpns-prevent-access-censored-websites-november
Deering, S. E., & Hinden, R. (1998). *Internet Protocol, Version 6 (IPv6) Specification*. Retrieved from http://tools.ietf.org/html/rfc2460
Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2010). *Access Controlled: The Shaping of*

Power, Rights, and Rule in Cyberspace - Google Books. Retrieved from https://books.google.com/books?id=ZojiQG4irWEC&pg=PA402&lpg=PA402&dq=Conroy+announces+mandatory+internet+filters+to+protect+children&source=bl&ots=HKr5bH_Dvi&sig=xkjYD-ZQD_7fpqtjYwp3QCUwFwI&hl=en&sa=X&ved=0ahUKEwiXqbbatYjTAhXFGpAKHRG5BQwQ6AEITjAJ#v=onepag

Delgado, E. (2014). Táchira amanece sin Internet por segundo día. *El Nacional*. Retrieved from http://www.el-nacional.com/regiones/Tachira-amanece-Internet-segundo-dia_0_359964053.html

Deloitte. (2016). *The economic impact of disruptions to Internet connectivity A report for Facebook*. Retrieved from http://globalnetworkinitiative.org/sites/default/files/The-Economic-Impact-of-Disruptions-to-Internet-Connectivity-Deloitte.pdf

Demirjian, K. (2015, January 15). Russia's culture minister calls for new 'patriotic Internet' to combat Western spin. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2015/01/15/russias-culture-minister-calls-for-new-patriotic-internet-to-combat-western-spin/?utm_term=.32d832dbc321

Denzin, Norma; Lincoln, Y. (2005). *The SAGE Handbook of Qualitative Research* (Y. Denzin, Norma; Lincoln, Ed.). Retrieved from http://www.amazon.com/The-SAGE-Handbook-Qualitative-Research/dp/0761927573

DeSoto, R. (2015). Court Orders DHS To Explain Legality Of Secret Plan To Shut Down Cell Service. Retrieved September 15, 2015, from WJ Western Journalism website: http://www.westernjournalism.com/court-orders-dhs-explain-legality-secret-plan-shut-cell-service/

DH. (2011). Cameron wanted to shut down Internet during riots: Report. Retrieved February 22, 2017, from Deccan Herald website: http://www.deccanherald.com/content/201981/cameron-wanted-shut-down-internet.html

DHS. (2013). Presidential Policy Directive/PPD-21. Retrieved March 27, 2016, from DHS website: http://fas.org/irp/offdocs/ppd/ppd-21.pdf

Diaz Hernandez, M. (2013). Venezuela: Internet blocked for three minutes on Election Day. Retrieved February 11, 2014, from Global Voices Advocacy website: http://advocacy.globalvoicesonline.org/2013/04/15/venezuela-internet-blocked-for-three-minutes-on-election-da/

Diaz, M. (2014). Venezuela: The Internet Goes Dark in Táchira. Retrieved October 26, 2015, from Global Voices Advocacy website: https://advox.globalvoices.org/2014/02/22/blackout-in-venezuela-the-internet-goes-dark-in-tachira-censorship-access/

Didymus, J. (2011, December). Australia: Internet services down due to Telstra outage. *Digital Journal*. Retrieved from http://digitaljournal.com/article/315865

Diniz, G., Muggah, R., & Glenny, M. (2014). Deconstructing cyber security in Brazil: Threats and Responses. *Strategic Paper*, (11), 1–35. Retrieved from https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf

Direitos Na Rede. (2017). Repudiation note On the attacks of the Temer government on the Internet Steering Committee in Brazil. Retrieved August 18, 2017, from Coalizao Direitos Na Rede website: https://direitosnarede.org.br/p/temers-government-attacks-cgi-br/

Ditz, J. (2015). White House Pushes to Keep Power to Shut Down Cellphone Networks. Retrieved September 15, 2015, from News from Antiwar.com website:

http://news.antiwar.com/2015/04/26/white-house-pushes-to-keep-power-to-shut-down-cellphone-networks/

Dogramaci, E., & Radcliffe, D. (2015). How Turkey Uses Social Media - Reuters Institute Digital News Report. Retrieved March 23, 2017, from Reuters Insititute website: http://www.digitalnewsreport.org/essays/2015/how-turkey-uses-social-media/

Dolgov, A. (2015a, January 14). Culture Minister Wants "Patriotic Internet" to Protect Russians. *The Moscow Times*. Retrieved from http://www.themoscowtimes.com/news/article/culture-minister-wants-patriotic-internet-to-protect-russians/514340.html

Dolgov, A. (2015b, January 15). Russian Culture Ministry Moves to Ban Films That Undermine "National Unity." *The Moscow Times*. Retrieved from http://www.themoscowtimes.com/news/article/russian-culture-ministry-moves-to-ban-films-that-undermine-national-unity/514440.html

Dou, D., Li, J., Qin, H., Kim, S., & Zhong, S. (2007). Understanding and Utilizing the Hierarchy of Abnormal BGP Events. *Proceedings of the Seventh Siam International Conference on Data Mining*, 467–472. Retrieved from http://apps.webofknowledge.com/full_record.do?product=WOS&search_mode=GeneralSearch&qid=7&SID=1DcqVo2Q1aEfMwrOSro&page=1&doc=1

Douglas, T. (2011). Social media's role in the riots. Retrieved August 8, 2017, from BBC News website: http://www.bbc.com/news/entertainment-arts-14457809

drupy2000. (2010). Chavez Quiere Regular (Censurar) El Internet En Venezuela. Retrieved from https://www.youtube.com/watch?v=Gne9CcoIHH4

Duckett, C. (2015). Australian Bureau of Meteorology tight-lipped on alleged Chinese hack. Retrieved November 11, 2017, from ZDNet website: http://www.zdnet.com/article/australian-bureau-of-meteorology-tight-lipped-on-alleged-chinese-hack/

Duffy, N. (2015). Internet freedom in Vladimir Putin's Russia: The noose tightens. Retrieved March 17, 2015, from AEI Research website: http://www.aei.org/publication/internet-freedom-vladimir-putins-russia-noose-tightens/

DUMA. (2014). Transcript on 17 October 2014. Retrieved February 26, 2016, from Duma Government of Russia website: http://transcript.duma.gov.ru/node/4154/

Dunn, A. (2011). Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising - ProQuest. *The Fletcher Forum of World Affairs*, *35*(2). Retrieved from http://search.proquest.com.libezproxy2.syr.edu/docview/874856828

Dunn Cavelty, M. (2008). *Cyber-security and threat politics US efforts to secure the information age*. Milton Park, Abingdon, Oxon ;;New York : Routledge,.

Dyn. (2012). Could It Happen In Your Country? Retrieved July 14, 2015, from Dyn Research | The New Home Of Renesys website: http://research.dyn.com/2012/11/could-it-happen-in-your-countr/

Dyn. (2014a). Brazil's Winning Internet. Retrieved March 11, 2017, from Dyn Blog website: http://dyn.com/blog/brazil-winning-internet/

Dyn. (2014b). Syria, Venezuela, Ukraine: Internet Under Fire. Retrieved October 1, 2014, from Dyn Research | The New Home Of Renesys website: http://research.dyn.com/2014/02/internetunderfire/#!prettyPhoto

Dyn. (2014c). The Resilient Internet: Why You Can't Shut It Down. Retrieved April 20, 2015, from Dyn Blog website: http://dyn.com/blog/the-resilient-internet-why-you-cant-shut-it-down/

Dyn. (2014d). Turkish Internet Censorship Takes a New Turn. Retrieved March 31, 2014, from Dyn Research | The New Home Of Renesys website: http://www.renesys.com/2014/03/turkish-internet-censorship/

Dyn. (2017). *Outages and Instabilities*. Retrieved from https://twitter.com/DynResearch

Eagleman, D. (2012). Four ways the Internet could go down. Retrieved March 20, 2014, from CNN Tech website: http://www.cnn.com/2012/07/10/tech/web/internet-down-eagleman/

Eckert, S. (2005). Protecting Critical Infrastructure: The Role of the Private Sector. Retrieved October 21, 2015, from ISN ETH Zurich website: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lang=en&id=21268

Economist. (2011, February). Reaching for the kill switch. The costs and practicalities of switching off the internet in Egypt and elsewhere. *The Economist*. Retrieved from http://www.economist.com/node/18112043

Economist. (2013, April). Shutting down the internet: Thou shalt not kill. *The Economist*. Retrieved from http://www.economist.com/news/special-report/21574633-turning-entire-internet-nuclear-option-best-not-exercised-thou-shalt-not-kill

EFE. (2015). Worrying Trend of Internet Shutdowns in Countries With Limited Connectivity. Retrieved September 1, 2015, from Electronic Frontier Foundation website: https://www.eff.org/deeplinks/2015/06/worrying-trend-shutting-internet-access-countries-limited-connectivity

EFE. (2017). Venezuelan opposition continues protests, death toll now at least 5. Retrieved April 13, 2017, from EFE website: http://www.efe.com/efe/english/portada/venezuelan-opposition-continues-protests-death-toll-now-at-least-5/50000260-3237633

EIU. (2007). The World in 2007 - The Economist Intelligence Unit's index of Democracy. Retrieved February 27, 2014, from The Economist website: file:///C:/Users/Pati/Documents/Pati/SYRACUSE/PhD/Proposal Defense/Regimes/DEMOCRACY_INDEX_2007_v3.pdf

EIU. (2008). The Economist Intelligence Unit's Index of Democracy 2008. Retrieved February 19, 2014, from The Economist website: http://graphics.eiu.com/PDF/Democracy Index 2008.pdf

EIU. (2011). Democracy index 2011. Democracy under stress. Retrieved March 1, 2014, from The Economist website: http://www.eiu.com/Handlers/WhitepaperHandler.ashx?fi=Democracy_Index_2011_Updated.pdf&mode=wp&campaignid=DemocracyIndex2011

EIU. (2016). Brazil Economy, Politics and GDP Growth Summary. Retrieved May 11, 2016, from The Economist Intelligence Unit website: http://country.eiu.com/brazil

EIU. (2017). Daily chart: Declining trust in government is denting democracy. Retrieved February 20, 2017, from The Economist Intelligence Unit website: http://www.economist.com/blogs/graphicdetail/2017/01/daily-chart-20

El Comercio. (2014, February). Venezuela: Táchira ya está militarizada y sin Internet. *El Comercio Perú*. Retrieved from http://elcomercio.pe/mundo/latinoamerica/venezuela-tachira-ya-esta-militarizada-y-sin-internet-noticia-1711107

El Comercio. (2016, February 18). Facebook: México crea vía para reportar amenazas recibidas en Facebook [Facebook: Mexico creates a channel to report threats received on Facebook]. *El Comercio Peru*. Retrieved from http://elcomercio.pe/redes-sociales/facebook/facebook-mexico-crea-via-reportar-amenazas-recibidas-facebook-noticia-1880188?ref=portada_home

El Nacional. (2017). Conatel prepara reglamento sobre uso de redes sociales. Retrieved August

18, 2017, from El Nacional website: http://www.el-nacional.com/noticias/gobierno/conatel-prepara-reglamento-sobre-uso-redes-sociales_185520

El Pais. (2010, March 15). Chávez dice que Internet "no puede ser libre." *El Pais - Archivo*. Retrieved from http://elpais.com/diario/2010/03/15/internacional/1268607606_850215.html

El Universal. (2014). Conatel bloqueó enlaces de... - Estilo de Vida [Conatel blocked Internet Connections]. Retrieved August 18, 2017, from El Universal website: http://www.eluniversal.com/noticias/estilo-vida/conatel-bloqueo-enlaces-internet_181005

El Universal. (2015, January 17). Servicio de Internet de Cantv reporta fallas [Cantv Internet service reports failures]. *El Universal*. Retrieved from http://www.eluniversal.com/nacional-y-politica/150117/servicio-de-internet-de-cantv-reporta-fallas

El19. (2013). Página del CNE ha recibido 45 mil ataques frustrados en una hora: Jorge Arreaza [CNE Webpage got 45 thousands frustrated attacks in one hour: Jorge Arreaza]. Retrieved October 26, 2015, from El 19 TV website: http://www.el19digital.com/articulos/ver/titulo:8087-pagina-del-cne-ha-recibido-45-mil-ataques-frustrados-en-una-hora-jorge-arreaza

Elinson, Z. (2011, August 20). After Cellphone Action, BART Faces Escalating Protests. *The New York Times*. Retrieved from http://www.nytimes.com/2011/08/21/us/21bcbart.html

Elinson, Z., & Walter, S. (2011, July 16). In San Francisco, Latest BART Shooting Prompts New Discussion of Reforms. *The New York Times*. Retrieved from http://www.nytimes.com/2011/07/17/us/17bcbart.html?scp=3&sq=zusha elinson bart&st=cse

EPIC. (2011). NCC Standard Operating Procedure (SOP) 303. Retrieved September 15, 2015, from epic website: http://epic.org/foia/dhs/internet-kill-switch/SOP-303-Redacted.pdf

EPIC. (2012). *FOIA Request to DHS*. Retrieved from https://perma.cc/Z7B5-83JK

EPIC. (2015). EPIC - EPIC v. DHS - SOP 303. Retrieved October 9, 2015, from Electronic Privacy Information Center website: https://epic.org/foia/dhs/internet-kill-switch/default.html

Eremenko, A. (2014a, September). Russia Speeds Up Law to Ban Most Foreign Web Services. *The Moscow Times*. Retrieved from http://www.themoscowtimes.com/news/article/russia-speeds-up-law-to-ban-most-foreign-web-services/507820.html

Eremenko, A. (2014b, December 2). Russia to Make Internet Providers Censor Content. *The Moscow Times*. Retrieved from http://www.themoscowtimes.com/article/russia-to-make-internet-providers-censor-content--report/512475.html

Espinoza, A. (2015). ¿Por qué se cayó el internet de CANTV por 12 horas? [Why CANTV Internet failed for 12 hours?]. Retrieved October 26, 2015, from El Estimulo website: http://elestimulo.com/blog/por-que-se-cayo-el-internet-de-cantv-por-12-horas/

European Commission. (2004). Critical Infrastructure Protection in the fight against terrorism. Retrieved from Lex Europa website: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0702&from=EN

Faratin, P., Clark, D., Gilmore, P., Bauer, S., Berger, A., & Lehr, W. (2007). *Complexity of Internet Interconnections: Technology, Incentives and Implications for Policy*. Retrieved from http://people.csail.mit.edu/wlehr/Lehr-Papers_files/Clark Lehr Faratin Complexity Interconnection TPRC 2007.pdf

Farid, F. Y. (2015). Algeria is shutting down the country's Internet up to 12 hours–for upgrades. Retrieved June 5, 2017, from Quartz website: https://qz.com/426367/algeria-shut-down-the-countrys-internet-up-to-12-hours-for-upgrades/

Farrell, H. (2013, November 11). Cyber-Pearl Harbor is a myth - The Washington Post. *The*

Washington Post. Retrieved from https://www.washingtonpost.com/news/monkey-cage/wp/2013/11/11/cyber-pearl-harbor-is-a-myth/?utm_term=.c611d5d54e56

Farrell, N. (2009). Australia's Internet goes down for an hour- The Inquirer. Retrieved September 10, 2015, from The Inquirer website: http://www.theinquirer.net/inquirer/news/1532262/australia-internet-goes-hour

Fink, A. (2010). *Conducting Research Literature Reviews - 3rd Ed. : From the Internet to Paper*. Retrieved from http://www.worldcat.org/title/conducting-research-literature-reviews-3rd-ed-from-the-internet-to-paper/oclc/785788342&referer=brief_results

Finol, J., & Espinoza, L. (2015). Los Derechos de Comunicacion en America Latina [Communication Rights in Latin America]. *Quórum Académico*, *12*(2). Retrieved from http://www.produccioncientificaluz.org/index.php/quorum/article/view/20454/20366

Fischer, E. (2012). Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions. Retrieved September 17, 2013, from Congressional Research Service website: http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-073.pdf

Fischer, E. A. (2014). *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*. Retrieved from https://fas.org/sgp/crs/natsec/R42114.pdf

Ford, P. (2014). Our Routers, Ourselves - The New Yorker. Retrieved September 16, 2015, from The New Yorker website: http://www.newyorker.com/tech/elements/our-routers-ourselves

Forrest Martin, F., Schnably, S. J., Wilson, R., Simon, J., & Tushnet, M. (2006). International Human Rights and Humanitarian Law: Treaties, Cases, and Analysis. Retrieved February 15, 2017, from Cambridge University Press website: https://books.google.com/books?id=sr9WSp3sih0C&pg=PA226&dq=ICCPR&hl=en&sa=X&ved=0ahUKEwjrmNaG55LSAhWrj1QKHf4HB6sQ6AEINzAF#v=onepage&q=ICCPR&f=false

Franceschi-Bicchierai, L. (2016). Turkey Doubles Down on Censorship With Block on VPNs, Tor. Retrieved November 7, 2016, from Motherboard website: https://motherboard.vice.com/read/turkey-doubles-down-on-censorship-with-block-on-vpns-tor

Francis, D. (2008). Russia threatens to build a separate Internet. Retrieved February 3, 2016, from Foreign Policy website: http://foreignpolicy.com/2008/01/03/russia-threatens-to-build-a-separate-internet/

Frankland, N. (2016). EOFY nightmare: businesses hit by Telstra outage. Retrieved September 13, 2016, from The New Daily website: http://thenewdaily.com.au/news/national/2016/06/30/telstra-outage-hits-businesses/

Frantz, E. (2011). *The politics of dictatorship : institutions and outcomes in authoritarian regimes*. Boulder Colo.: Lynne Rienner Publishers.

Galperin, E., & O'brien, D. (2016). Russia Asks For The Impossible With Its New Surveillance Laws. Retrieved March 15, 2017, from Electronic Frontier Foundation website: https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws

Galperina, M. (2016). Putin Is Literally Breaking The Internet. Retrieved July 8, 2016, from GAWKER website: http://gawker.com/putin-is-literally-breaking-the-internet-1783293408?utm_campaign=socialflow_gawker_twitter&utm_source=gawker_twitter&utm_medium=socialflow

Garcia Martinez, A. (2014). Propuesta de Peña Nieto criminaliza uso de internet: activistas. Retrieved October 22, 2014, from Cimac Noticias website: http://cimacnoticias.com.mx/node/66098

Geddes, B. (2004). Minimum-Winning Coalitions and Personalization in Authoritarian Regimes. *Annual Meetings of the American Political Science Association*. Retrieved from http://www.international.ucla.edu/cms/files/geddes.pdf

Gellman, B., Blake, A., & Miller, G. (2013, June 9). Edward Snowden comes forward as source of NSA leaks. *The Washington Post*. Retrieved from https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?utm_term=.ad7ddd9afba4

Germano, J. H. (2014). *Cybersecurity Partnerships: A New Era of Public-Private Collaboration*. Retrieved from http://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf

Ghosh, P. (2011). David Cameron Wanted Internet Shutdown During Britain's Summer Riots. Retrieved February 12, 2014, from International Business Times website: http://www.ibtimes.com/david-cameron-wanted-internet-shutdown-during-britains-summer-riots-364002

Giacomello, G. (2005). *National Governments and Control of the Internet: A Digital Challenge (Routledge Research in Information Technology and Society)*. Routledge.

Giacomello, G. (2016). The Perfect Storm. *International Studies Association Annual Conference*. Atlanta, Ga.

Gibbs, S. (2004). Cuba law tightens internet access. Retrieved March 9, 2014, from BBC NEWS | Americas | website: http://news.bbc.co.uk/2/hi/americas/3425425.stm

GNI. (2018). Human Rights and Net Disruptions - Global Network Initiative. Retrieved August 6, 2018, from Global Network Initiative website: https://globalnetworkinitiative.org/disconnected-human-rights-network-disruptions/

Goldman, D. (2015). Donald Trump wants to "close up" the Internet. Retrieved December 9, 2015, from CNN Money website: http://money.cnn.com/2015/12/08/technology/donald-trump-internet/

Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet? : illusions of a borderless world*. New York: Oxford University Press.

Golitsyn, A. (2014a, September 19). Security Council to discuss off Russia from the global Internet. *Vedomosti.RU*. Retrieved from http://www.vedomosti.ru/politics/articles/2014/09/19/suverennyj-internet#cut

Golitsyn, A. (2014b, September 19). STATEMENTS - The Security Council will discuss the shutdown of Russia from the global Internet. *Vedomosti.RU*. Retrieved from http://www.vedomosti.ru/politics/news/33610271/suverennyj-internet

Golitsyn, A., Sergina, E., & Kozlov, P. (2016, February 11). The government wants to control the routes Internet traffic in the country. *Vedomosti*. Retrieved from http://www.vedomosti.ru/politics/articles/2016/02/11/628508-gosudarstvo-hochet-kontrolirovat-rossiiskii-zarubezhnii-internet-trafik-strane

Golitsyna, A., Sergina, E., & Kozlov, P. (2016). Государство хочет контролировать маршруты интернет-трафика в стране [The State Wants to Control the Routes of Internet Traffic in the Country]. Retrieved November 7, 2018, from Ведомости [Vedomosti] website: https://www.vedomosti.ru/politics/articles/2016/02/11/628508-gosudarstvo-hochet-kontrolirovat-rossiiskii-zarubezhnii-internet-trafik-strane

Gomez, A. (2013). Apagón del servicio de Internet de Cantv generó suspicacias [Internet shutdown generated mistrusts]. Retrieved October 2, 2015, from El Mundo website:

http://www.elmundo.com.ve/noticias/tecnologia/internet/apagon-del-servicio-de-internet-de-cantv-genero-su.aspx

Gonzales, D., & Harting, S. (2011). Can You Hear Libya Now? - NYTimes.com. *The New York Times*. Retrieved from http://www.nytimes.com/2011/03/05/opinion/05Gonzales.html?scp=1&sq=Dan Gonzales Libya&st=cse&_r=0

Gonzalo, M. (2010). La Ley Resorte en Venezuela: una ley para controlar internet. Retrieved from hipertextual website: https://hipertextual.com/2010/12/la-ley-resorte-en-venezuela-una-ley-para-controlar-internet

Google. (2011). Download data – Google Transparency Report. Retrieved February 7, 2014, from Google website: http://www.google.com/transparencyreport/traffic/data/

GOV.UK. (2012). Parents asked if adult websites should be blocked - GOV.UK. Retrieved February 4, 2018, from GOV.UK website: https://www.gov.uk/government/news/parents-asked-if-adult-websites-should-be-blocked

Govtrack.us. (2010). Protecting Cyberspace as a National Asset Act of 2010 (2010; 111th Congress H.R. 5548). Retrieved February 22, 2017, from GovTrack.us website: https://www.govtrack.us/congress/bills/111/hr5548

GPO. (2010). S.773 (RS) - Cybersecurity Act of 2009. Retrieved August 13, 2017, from U.S. Government Publishing Office website: https://www.gpo.gov/fdsys/pkg/BILLS-111s773rs

Greenber, M. H. (2003). A Return to Lilliput: The LICRA v. Yahoo - Case and the Regulation of Online Content in the World Market. *Berkeley Tech. L.J. 1191*, *18*(4), 1197–1258.

Greenfield, R. (2018). Authoritarian ICO: How Venezuela's Government Is Abusing the Blockchain. Retrieved March 16, 2018, from consensys website: https://media.consensys.net/authoritarian-ico-how-venezuelas-government-is-abusing-the-blockchain-a7a9b8275aa6

Greenwald, G., MacAskill, E., & Poitras, L. (2013). Edward Snowden: the whistleblower behind the NSA surveillance revelations. Retrieved March 17, 2018, from The Guardian website: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Grossi, B. (2014). Brazilian Judge intends to shut down facebook.com. Retrieved September 3, 2015, from Defero Law website: http://www.deferolaw.com/news/brazilian-judge-intends-to-shut-down-facebook-com/

Grygiel, J. (2016). The Return of Europe's Nation-States. Retrieved November 16, 2016, from Foreign Affairs website: https://www.foreignaffairs.com/articles/europe/return-europe-s-nation-states

Gurdus, E. (2016). We're headed for a "cyber Pearl Harbor," says Adm James Stavridis. Retrieved February 18, 2017, from CNBC website: http://www.cnbc.com/2016/12/15/were-headed-at-a-cyber-pearl-harbor-says-adm-james-stavridis.html

Hale, H. E. (2010). Eurasian polities as hybrid regimes: The case of Putin's Russia. *Journal of Eurasian Studies*, *1*(1), 33–41. https://doi.org/10.1016/j.euras.2009.11.001

Halliday, J. (2011a). London riots: how BlackBerry Messenger played a key role. Retrieved August 8, 2017, from theguardian website: https://www.theguardian.com/media/2011/aug/08/london-riots-facebook-twitter-blackberry

Halliday, J. (2011b, August 11). David Cameron considers banning suspected rioters from social media. *The Guardian*. Retrieved from https://www.theguardian.com/media/2011/aug/11/david-cameron-rioters-social-media

Hansen, L. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175.

Harding, L. (2014, September 19). Putin considers plan to unplug Russia from the internet "in an emergency." *The Guardian*. Retrieved from http://www.theguardian.com/world/2014/sep/19/vladimir-putin-plan-unplug-russia-internet-emergency-kremlin-moscow

Harding, N. (2011). Could the UK Government shut down the web? Retrieved February 28, 2016, from The Independent website: https://www.independent.co.uk/life-style/gadgets-and-tech/features/could-the-uk-government-shut-down-the-web-2235116.html

Hardings, N. (2011). Could the UK Government shut down the web? Could the UK Government shut down the web? - Features - Gadgets & Tech - The Independent.

Harlow, S., & Johnson, T. (2011a). Overthrowing the Protest Paradigm? How The New York Times, Global Voices and Twitter Covered the Egyptian Revolution. Retrieved October 8, 2012, from International Journal of Communication website: http://ijoc.org/ojs/index.php/ijoc/article/viewFile/1239/611

Harlow, S., & Johnson, T. J. (2011b, September 2). The Arab Spring| Overthrowing the Protest Paradigm? How The New York Times, Global Voices and Twitter Covered the Egyptian Revolution. *International Journal of Communication*, Vol. 5, p. 16. Retrieved from http://ijoc.org/index.php/ijoc/article/view/1239

Harman, J. *All Info - H.R.5548 - 111th Congress (2009-2010): Protecting Cyberspace as a National Asset Act of 2010*. , (2010).

Harvey, N. (MP). (2011). Cyber security in the UK. Retrieved September 11, 2015, from Speeches - GOV.UK website: https://www.gov.uk/government/speeches/2011-11-21-cyber-security-in-the-uk

Hassanpour, N. (2014, March 23). Erdogan's Twitter flail -. *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/03/23/erdogans-twitter-flail/

Hautala, L. (2015). Donald Trump wants to shut off the Internet. Retrieved from CNET website: http://www.cnet.com/news/donald-trump-wants-to-shut-down-the-internet/

Havyatt, D. (2011). Analysis: The legal means to cut net access. Retrieved February 24, 2016, from Networking - Security - Telco/ISP - iTnews website: http://www.itnews.com.au/news/analysis-the-legal-means-to-cut-net-access-246949

Hernandez, V. (2014). Telstra 4G Coverage To Reach 90% Of Australia By End Of January 2016. Retrieved December 19, 2016, from International Bussiness Times website: http://www.ibtimes.com.au/telstra-4g-coverage-reach-90-australia-end-january-2016-1368929

Hernando, C. (2015). CNN Final Presidential Debate Donald Trump Shut down internet Free speech foolish. Retrieved from https://www.youtube.com/watch?v=JcmiHx5Yf2I

Herrero, A. V. (2019, February 4). In Fight for Venezuela, Who Supports Maduro and Who Backs Guaidó? *The New York Times*. Retrieved from https://www.nytimes.com/2019/02/04/world/americas/venezuela-support-maduro-guaido.html

Hewitt, K. (2016). 2 Ways an Entire Country Can Lose Access to the Internet-and Why the U.S. is Resistant - The Akamai Blog. Retrieved July 31, 2017, from Akamai website: https://blogs.akamai.com/2016/10/2-ways-an-entire-country-can-lose-access-to-the-internet-and-why-the-us-is-resistant.html

Hill, E. (2011). Conditions in Libya deteriorating. Retrieved March 11, 2014, from Aljazeera2

website: http://www.aljazeera.com/indepth/spotlight/libya/2011/03/201134162742713130.html

Hille, K. (2015). Twitter told to store Russian data in Russia. Retrieved June 9, 2017, from Financial Times website: https://www.ft.com/content/e04e035c-87c6-11e5-90de-f44762bf9896

Hiller, J. (2002). *Internet law & policy*. Upper Saddle River N.J.: Prentice Hall.

History.com. (2009). Blitzkrieg. Retrieved March 17, 2018, from History Channel -A + E Networks website: https://www.history.com/topics/world-war-ii/blitzkrieg

HM Government. (2016). *National Cyber Security Strategy 2016-2021*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Hoefer, R. (2012). *Policy creation and evaluation : understanding welfare reform in the United States*. New York: Oxford University Press.

Hoffman, C. (2016). HTG Explains: What is DNS Cache Poisoning? Retrieved September 21, 2015, from How-To-Geek website: http://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/

Holmes, R. (2013). The Future Of Social Media? Forget About The U.S., Look To Brazil. Retrieved March 24, 2017, from Forbes website: https://www.forbes.com/sites/ciocentral/2013/09/12/the-future-of-social-media-forget-about-the-u-s-look-to-brazil/#69138f013c9a

Homeland Security & Governmental Affairs Committee. (2010). LIEBERMAN, COLLINS, CARPER UNVEIL MAJOR CYBERSECURITY BILL TO MODERNIZE, STRENGTHEN, AND COORDINATE CYBER DEFENSES. Retrieved October 21, 2015, from Homeland Security and Governmental Affairs website: https://www.hsgac.senate.gov/media/majority-media/lieberman-collins-carper-unveil-major-cybersecurity-bill-to-modernize-strengthen-and-coordinate-cyber-defenses

Hopkins, C. (2015). A timeline of Hugo Chávez's harsh, anti-free speech actions. Retrieved September 17, 2017, from The Daily Dot website: https://www.dailydot.com/layer8/hugo-chavez-anti-free-speech-actions/

Horvath, D. J., & Daly, D. J. (1989). *Small Countries in the World Economy: The Case of Sweden : What Canada Can Learn from the Swedish Experience*. Inst for Research on.

Horvitz, R. (2013). *Geo-Database Management of White Space vs. Open Spectrum*. Retrieved from http://papers.ssrn.com/abstract=2279099

Howard, P., Agarwal, S., & Hussain, M. (2011). The Dictator's Digital Dilemma: When Do States Disconnect their Digital Networks? *Issues in Technology Innovation*, (13).

Howard, P. N., Agarwal, S. D., & Hussain, M. M. (2011). The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks? Regime Responses to the Political Use of Social Media. *Issues in Technology Innovation*, (13). Retrieved from https://www.brookings.edu/wp-content/uploads/2016/06/10_dictators_digital_network.pdf

Howard, P. N., & Hussain, M. M. (2013). *Democracy's Fourth Wave?: Digital Media and the Arab Spring (Oxford Studies in Digital Politics)*. Oxford University Press, USA.

HTB. (2014). ков успокоил россиян на тему отключения Рунета от мировой Сети [Sands reassured Russians to disable the theme of Runet World Network]. Retrieved February 26, 2016, from HTB website: http://www.ntv.ru/novosti/1216980/

Hunt, E. (2016). Telstra says system shutdown was due to "embarrassing human error." Retrieved June 22, 2016, from The Guardian website:

https://www.theguardian.com/business/2016/feb/09/telstra-customers-lose-phone-and-internet-services-in-mass-systems-failure

HwCol. (2014). Venezuela apaga sus servicios de internet por orden del gobierno [Venezuelan Government Shuts Down Internet Services]. Retrieved March 19, 2017, from HwCol website: http://hwcol.com/2014/02/22/venezuela-apaga-sus-servicios-de-internet-por-orden-del-gobierno/

ICJ. (1949). *Reparation for Injuries Suffered in the Service of the United Nations. Advisory Opinion of 11 April 1949.* Retrieved from http://www.icj-cij.org/docket/files/4/1837.pdf

ICJ. (2017). The Court. Retrieved February 14, 2017, from International Court of Justice website: http://www.icj-cij.org/court/index.php?p1=1

IMF. (2014). International Monetary Fund Home Page. Retrieved April 21, 2014, from IMF-International Monetary Fund Home Page website: http://www.imf.org/external/index.htm

Inkeles, A. (1991). *On Measuring Democracy: Its Consequences and Concomitants*. Retrieved from http://books.google.com/books?id=uxO2QHFzlZsC&pg=PA110&dq=a+combination+of+appeals+to+traditional+legitimacy,+patron-client+ties,+and+repression&hl=en&sa=X&ei=EJEUU6fKGcSYrAGh9IDQDw&ved=0CCsQ6AEwAA#v=onepage&q=a combination of appeals to traditional legitimacy%2C patron-client ties%2C and repression&f=false

Ionescu, D. (2011). UK Considers Cutting Off Twitter, BlackBerry During Riots. Retrieved April 30, 2014, from PCW website: http://www.pcworld.com/article/237858/uk_considers_cutting_off_twitter_blackberry_during_riots.html

IPYS. (2017). Nuevo Estado de Excepción Contempla "Regulaciones Contundentes" a los Contenidos en Internet [New State of Emergency Contains "Blunt Regulations" to the Internet Content]. Retrieved August 17, 2017, from Instituto Prensa y Sociedad Venezuela - IPYS website: http://ipysvenezuela.org/alerta/nuevo-estado-excepcion-contempla-regulaciones-contundentes-los-contenidos-internet/

Ismail, N. (2017). Ethiopia's internet shut down by government. Retrieved June 5, 2017, from Information Age website: http://www.information-age.com/ethiopias-internet-shut-down-government-123466566/

ISOC. (2011). Egypt Internet Shutdown Q&A. Retrieved March 11, 2014, from Internet Society website: http://www.internetsociety.org/articles/egypt-internet-shutdown-qa

ISOC. (2012). *Promoting the use of Internet Exchange Points (IXPs) A Guide to Policy, Management and Technical Issues*. Retrieved from https://www.internetsociety.org/sites/default/files/Promoting the use of IXPs.pdf

ISOC. (2017a). ISOC está profundamente preocupada por los bloqueos de Internet en Venezuela [ISOC is Deeply Worried Because of the Internet Blocking Episodes in Venezuela]. Retrieved August 16, 2017, from Internet Society website: https://www.isocvenezuela.org/isoc-esta-profundamente-preocupada-por-los-bloqueos-de-internet-en-venezuela/

ISOC. (2017b). Policy Brief: Internet Shutdowns. Retrieved January 15, 2018, from Internet Society website: https://www.internetsociety.org/policybriefs/internet-shutdowns

IT News Africa. (2017). Ethiopia shuts down internet ahead of exams. Retrieved June 5, 2017, from IT News Africa website: https://www.itnewsafrica.com/2017/06/ethiopia-shuts-down-internet-ahead-of-exams/

ITS Rio. (2016). Políticos querem censurar a internet no Brasil com a desculpa de combater o

"cibercrime" — Medium. Retrieved March 31, 2016, from ITS Rio website: https://medium.com/@ITSriodejaneiro/políticos-querem-censurar-a-internet-no-brasil-com-a-desculpa-de-combater-o-cibercrime-bb2de118efa3#.2fjlj93nb

Jacobs, D. (2013). Internet kill switch: Government might have to disclose its Standard Operating Procedure 303 policy. Retrieved from Future Tense website: http://www.slate.com/blogs/future_tense/2013/11/25/internet_kill_switch_government_might_have_to_disclose_its_standard_operating.html

Johnson, B. (2011). How Egypt Switched Off the Internet. Retrieved March 11, 2014, from GIGAOM website: http://gigaom.com/2011/01/28/how-egypt-switched-off-the-internet/

Johnson, M. (2011). The "internet kill switch" debate: Knocking over entire web systems. *The Economist*. Retrieved from http://www.economist.com/blogs/multimedia/2011/02/internet_kill_switch_debate

Johnston, C. (2016). Russia PM warns of "new cold war" amid Syria accusations. Retrieved February 14, 2016, from The Guardian website: http://www.theguardian.com/world/2016/feb/13/russia-warns-of-new-cold-war-amid-syria-accusations-munich

Jones, K. (2005). Nepal: Out of the Silence - Reports - Committee to Protect Journalists. Retrieved April 3, 2014, from CPJ Committee to Protect Journalists website: https://cpj.org/reports/2005/05/nepal-news.php

Jones, S., Sevastopulo, D., & Hille, K. (2016). Democrats hacked: Russia trail sees Moscow accused of wider aims. Retrieved July 26, 2016, from Financial Times website: https://next.ft.com/content/6e0b9a84-5278-11e6-befd-2fc0c26b3c60

Jr., M. H., Lawson, S., & McFarlane, M. D. (2015). *The Rhetorical Invention of America's National Security State*. Retrieved from https://books.google.com/books?id=teAXCgAAQBAJ&pgis=1

Jutila, M. (2015). Securitization, history, and identity: some conceptual clarifications and examples from politics of Finnish war history. *Nationalities Papers*, *43*(6), 927–943. https://doi.org/10.1080/00905992.2015.1065402

Kafka, P., & Molla, R. (2017). Comcast, the largest broadband company in the U.S., is getting even bigger. Retrieved November 12, 2018, from recode website: https://www.recode.net/2017/4/27/15413870/comcast-broadband-internet-pay-tv-subscribers-q1-2017

Kantyshev, P., & Sergina, E. (2017, August 17). The Russian authorities are preparing new restrictions for foreigners. *Vedomosti*. Retrieved from https://www.vedomosti.ru/technology/articles/2017/08/17/729810-vlasti-gotovyat-ogranicheniya-inostrantsev

Karanja, M., Xynou, M., & Filasto, A. (2016). Ethiopia's protests were stifled by a coordinated internet shutdown — Quartz. Retrieved August 14, 2016, from Quartz website: http://qz.com/757824/how-the-ethiopia-protests-were-stifled-by-a-coordinated-internet-shutdown/

Katzenstein, P. J. (2003). Same War—Different Views: Germany, Japan, and Counterterrorism. *International Organization*, *57*(04), 731–760. Retrieved from http://journals.cambridge.org/abstract_S0020818303574033

Keane, B. (2012a). National security inquiry proposals internet kill switch and individuals. Retrieved September 1, 2015, from CRIKEY website: http://www.crikey.com.au/2012/09/10/what-is-the-government-up-to-on-australias-internet-

kill-switch/
Keane, B. (2012b). What is the government up to on Australia's internet kill switch? Retrieved September 8, 2016, from CRIKEY website: https://www.crikey.com.au/2012/09/10/what-is-the-government-up-to-on-australias-internet-kill-switch/
Keating, J. (2013a). Brazilian President Dilma Rousseff slams U.S. surveillance at the United Nations: Responding to spying allegations with a call for Internet sovereignty. Retrieved June 24, 2015, from The World website: http://www.slate.com/blogs/the_world_/2013/09/24/brazilian_president_dilma_rousseff_slams_u_s_surveillance_at_the_united.html
Keating, J. (2013b). Rouseff's Cybernationalism. Retrieved January 1, 2015, from Slate website: http://www.slate.com/blogs/the_world_/2013/09/24/brazilian_president_dilma_rousseff_slams_u_s_surveillance_at_the_united.html
Keith, L. (1999). The United Nations International Covenant on Civil and Political Rights : does it make a difference in human rights behavior? *Journal of Peace Research*, *36*(1), 95–118.
Kerr, D. (2014). Bloquea Internet el gobierno de Venezuela? Retrieved January 1, 2015, from CNET website: http://www.cnet.com/es/noticias/bloquea-internet-el-gobierno-de-venezuela/
Khan, D.-E. (2007). Max Huber as Arbitrator: The Palmas (Miangas) Case and Other Arbitrations. *European Journal of International Law*, *18*(1), 145–170. https://doi.org/10.1093/ejil/chm011
Khondker, H. H. (2011). Role of the New Media in the Arab Spring. *Globalizations*, *8*(5), 675–679. https://doi.org/10.1080/14747731.2011.621287
Kidman, A., & Allen, D. (2012). Telstra Lost The Internet, Not Sure Why. Retrieved April 23, 2014, from Gizmodo Australia website: http://www.gizmodo.com.au/2012/02/telstra-lost-the-internet-not-sure-why/
Kiernan, S. (2016). Telstra outage hits 75,000 broadband customers. Retrieved June 13, 2016, from CRN website: http://www.crn.com.au/news/telstra-outage-hits-75000-broadband-customers-420705
Kizilkaya, E. (2014). Turkey's new Internet law contradicts its EU ambitions - Al-Monitor: the Pulse of the Middle East. Retrieved December 28, 2014, from ALMONITOR website: http://www.al-monitor.com/pulse/originals/2014/09/turkey-european-union-internet-law-human-rights.html#
Klausen, A.-L., & Humphry, E. (2015). What is a fragile state? Retrieved February 17, 2017, from The World Bank website: http://blogs.worldbank.org/developmenttalk/what-fragile-state
Klemm, D., & Johnson, D. (2010). *National Risk Management Policy and Framework for National Security Systems*.
Knapp, E. (2011). *Industrial network security : securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems*. Retrieved from https://books.google.com/books?hl=en&lr=&id=V2RzAwAAQBAJ&oi=fnd&pg=PP1&dq=isolate+critical+infrastructure&ots=53wcWdnvmm&sig=lYIHPWdO_t7ENOv8CZEt9UssL4#v=onepage&q=isolate&f=false
Koerber, R. (2016). Yet Another Telstra Outage Hits Customers, And They Are Pissed. Retrieved September 13, 2016, from The Huffington Post website: http://www.huffingtonpost.com.au/2016/06/30/yet-another-telstra-outage-hits-customers-and-they-are-pissed/
Kolb, R. (2013). *The International Court of Justice*. Retrieved from https://books.google.com/books?id=SpjbBAAAQBAJ&printsec=frontcover&dq=ICJ&hl=en&sa=X&ved=0ahUKEwi3o8XEtZDSAhUPyWMKHfOJBxUQ6AEIHDAA#v=onepage&

q=ICJ&f=false
Kolomychenko, M., & Kommersant. (2016). The Russian internet ranks among the world's most stable. Retrieved June 13, 2016, from Russia Beyond the Headlines website: http://rbth.com/science_and_tech/2016/06/08/the-russian-internet-ranks-among-the-worlds-most-stable_601341
Korsunskaya, D., & Winning, A. (2016). Russian ministry eyes $16 billion in privatizations in 2017-19 | Reuters. Retrieved March 20, 2017, from REUTERS website: http://www.reuters.com/article/us-russia-economy-privatisation-idUSKBN12X1NG?il=0
Koshkin, P. (2014, September). The Kremlin gives the green light to shut down the Internet. *Russia Direct*. Retrieved from http://www.russia-direct.org/analysis/kremlin-gives-green-light-shut-down-internet
Kramer, A. E. (2014a, October 1). Putin Supports Project to 'Secure' Russia Internet. *The New York Times*. Retrieved from http://www.nytimes.com/2014/10/02/world/europe/russia-vladimir-putin-internet.html?_r=0
Kramer, A. E. (2014b, October 1). Putin Supports Project to 'Secure' Russia Internet. *The New York Times*. Retrieved from http://www.nytimes.com/2014/10/02/world/europe/russia-vladimir-putin-internet.html
Kravets, D. (2015a). Court won't force US to divulge secret strategy to cut mobile phone service. Retrieved September 15, 2015, from Ars Technica LAW & DISORDER / CIVILIZATION & DISCONTENTS website: http://arstechnica.com/tech-policy/2015/05/court-wont-force-us-to-divulge-secret-strategy-to-cut-mobile-phone-service/
Kravets, D. (2015b). Will Supreme Court force DHS to divulge secret plan to cut cell service? Retrieved February 16, 2016, from Ars Technica LAW & DISORDER / CIVILIZATION & DISCONTENTS website: http://arstechnica.com/tech-policy/2015/08/will-supreme-court-force-dhs-to-divulge-secret-plan-to-cut-cell-service/
Kravets, D. (2016). Supreme Court won't force DHS to reveal secret plan to cut cell service | Ars Technica. Retrieved January 3, 2017, from Ars Technica website: http://arstechnica.com/tech-policy/2016/01/supreme-court-wont-force-dhs-to-reveal-secret-plan-to-cut-cell-service/
Krieger, M. (2015). Britain's "War on Terror" Insanity Continues – David Cameron Declares War on Encryption. Retrieved July 15, 2015, from Liberty Blitzkrieg website: http://libertyblitzkrieg.com/2015/01/12/britains-war-on-terror-insanity-continues-david-cameron-declares-war-on-encryption/
Krieger, M. (2017). UK Government Moves Aggressively to Censor and Control the Internet. Retrieved August 29, 2017, from Liberty Blitzkrieg website: https://libertyblitzkrieg.com/2017/05/19/uk-government-moves-aggressively-to-censor-and-control-the-internet/
Ku, J. G. (2010). Unitary Executive Theory and Exclusive Presidential Powers. *University of Pennsylvania Journal of Constitutional Law*, *12*(2), 615–621. Retrieved from https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1124&context=jcl
Kulesza, J. (2012). *International Internet law*. Retrieved from http://www.worldcat.org/title/international-internet-law/oclc/724640168&referer=brief_results
LaCapria, K. (2015). All Your Facebook are Belong to Trump. Retrieved February 3, 2016, from snopes.com website: http://www.snopes.com/trump-wants-shut-internet/
Latif Dahir, A. (2017). Ethiopia shut down the internet ahead of a scheduled. Retrieved June 5,

2017, from Quartz website: https://qz.com/994990/ethiopia-shut-down-the-internet-ahead-of-a-scheduled-countrywide-national-exams/

Lawfare. (2014). Snowden Revelations. Retrieved March 14, 2017, from Lawfare website: https://www.lawfareblog.com/snowden-revelations

Lawson, S. (2011). Is America Really Building An Internet "Kill Switch." Retrieved September 14, 2015, from Forbes website: http://www.forbes.com/sites/firewall/2011/02/11/is-america-really-building-an-internet-kill-switch/

Lawson, S. (2016). Does 2016 Mark the End of Cyber Pearl Harbor Hysteria? Retrieved February 17, 2017, from Forbes website: https://www.forbes.com/sites/seanlawson/2016/12/07/does-2016-mark-the-end-of-cyber-pearl-harbor-hysteria/#4194c33322c2

Lehtinen, R., Russell, D., & Gangemi Sr., G. T. (2012). *Computer Security Basics* (2nd ed.; T. Apandi, Ed.). Sebastopol CA: O'Reilly Media, Inc.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., … Wolff, S. (1997). Brief History of the Internet. Retrieved November 4, 2017, from Internet Society website: https://www.internetsociety.org/internet/history-internet/brief-history-internet/

LeMay, R. (2010a). Govt doesn't trust "internet companies", says Conroy. Retrieved February 24, 2016, from Delimiter website: https://delimiter.com.au/2010/07/09/govt-doesnt-trust-internet-companies-says-conroy/

LeMay, R. (2010b). Internet association slams Conroy's "personal attacks" . Retrieved February 24, 2016, from Delimiter website: https://delimiter.com.au/2010/05/28/internet-association-slams-conroys-personal-attacks/

LeMay, R. (2011). No internet "kill switch" for Australia, says Conroy - Delimiter. Retrieved September 30, 2014, from Delimiter website: http://delimiter.com.au/2011/02/03/no-internet-kill-switch-for-australia-says-conroy/

LeMay, R. (2012). Conroy fights Internet control in Dubai. Retrieved February 24, 2016, from Delimiter website: https://delimiter.com.au/2012/12/03/conroy-fights-internet-control-in-dubai/

Leskin, P. (2017). On Net Neutrality, Here's What AT&T, Verizon, Charter, and Comcast Say. Retrieved December 11, 2017, from Inverse Innovation website: https://www.inverse.com/article/38734-net-neutrality-att-verizon-charter-comcast

Lieberman. *Titles S.3480 - 111th Congress (2009-2010): Protecting Cyberspace as a National Asset Act of 2010.* , (2010).

Lieberman, J. I. (2011a). *Opening Statement of Chairman Joseph Lieberman "Protecting Cyberspace: Assessing the White House Proposal" Homeland Security and Governmental Affairs Committee*. Retrieved from http://hsgac.senate.gov

Lieberman, J. I. (2011b, February 17). *Bill Summary & Status 112th Congress (2011 - 2012) S.413*. Retrieved from http://thomas.loc.gov/cgi-bin/bdquery/z?d112:SN00413:@@@D&summ2=m&

Linz, J. (2000). *Totalitarian and authoritarian regimes*. Boulder CO: Lynne Rienner Publishers.

Lipman, M. (2014). Putin's Fear of the Internet. Retrieved September 17, 2017, from The New Yorker website: https://www.newyorker.com/news/news-desk/putins-fear-of-the-internet

Lohman, T. (2011). Can Australia's internet be switched off, too? - Computerworld. Retrieved April 22, 2014, from COMPUTERWORLD website: http://www.computerworld.com.au/article/374883/can_australia_internet_switched_off_too_/

Lokot, T. (2014). This Russian Lawmaker Thinks the US Can Take Russia Off The Internet.

Retrieved February 26, 2016, from Global Voices website: https://globalvoices.org/2014/09/06/us-russia-internet-cut-blackout-security/

Lomas, N. (2016). Yes, the U.K. now has a law to log web users' browsing behavior, hack devices and limit encryption. Retrieved December 19, 2016, from TechCrunch website: https://techcrunch.com/2016/11/29/yes-the-uk-now-has-a-law-to-log-web-users-browsing-behavior-hack-devices-and-limit-encryption/

Lotan, G. ., & Graeff, E. . (2011). The Revolutions Were Tweeted: Information Flows during the 2011 Tunisian and Egyptian Revolutions. *International Journal of Communications*, (5), 1375–1405. Retrieved from http://ijoc.org/ojs/index.php/ijoc/article/view/1246

Lucas, N., & Juarez, C. (2018). AT&T competirá a Telmex, Izzi y Megacable el mercado del internet fijo. Retrieved November 6, 2018, from El Economista website: https://www.eleconomista.com.mx/empresas/ATT-competira-a-Telmex-Izzi-y-Megacable-el-mercado-del-internet-fijo-20180416-0032.html

Lunden, I. (2016). LinkedIn is now officially blocked in Russia. Retrieved September 20, 2017, from TechCrunch website: https://techcrunch.com/2016/11/17/linkedin-is-now-officially-blocked-in-russia/

MacAskill, E. (2014). Putin calls internet a "CIA project" renewing fears of web breakup. Retrieved April 24, 2014, from The Guardian website: http://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia

Macdonald, C. (2017). Russia plans to create an "independent internet" by 2018. Retrieved January 27, 2018, from Daily Mail Online website: http://www.dailymail.co.uk/sciencetech/article-5126931/Russia-plans-create-independent-internet-2018.html

MacFarquhar, N. (2014, May 6). Russia Quietly Tightens Reins on Web With 'Bloggers Law' - The New York Times. *The New York Times*. Retrieved from https://www.nytimes.com/2014/05/07/world/europe/russia-quietly-tightens-reins-on-web-with-bloggers-law.html

MacKinnon, R. (2012). *Consent of the networked : the world-wide struggle for Internet freedom*. New York: Basic Books.

Madori, D. (2015). The Threat of Telecom Sabotage - Dyn Research. Retrieved November 9, 2015, from The New Home Of Renesys website: http://research.dyn.com/2015/10/the-threat-of-telecom-sabotage/

Madory, D. (2014). No turning back: Russia activates Crimean cable. Retrieved October 1, 2014, from Dyn Research | The New Home Of Renesys website: http://research.dyn.com/2014/07/no-turning-back-russia-crimea/

Mandarino Junior, R., & Canongia, C. (2010). *Livro Verde Seguranca Cibernetica No Brasil [Green Book of Cyber-Security in Brazil]*. Retrieved from http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf

Markoff, J. (2015, December 8). Why Donald Trump's Call to "Close Up" the Internet is Science Fiction. *The New York Times*. Retrieved from https://bits.blogs.nytimes.com/2015/12/08/why-donald-trumps-call-to-close-up-the-internet-is-science-fiction/?_r=0

Marsden, C. (2011). The Internet kill-switch: UK law. Retrieved February 11, 2014, from Internet Law Sussex website: http://internetsussex.blogspot.com/2011/03/internet-kill-switch-uk-law.html

Martinez, L. A. (2018). 7 gráficos sobre los usuarios de internet en México en 2018. Retrieved November 6, 2018, from El Economista website:

https://www.eleconomista.com.mx/tecnologia/7-graficos-sobre-los-usuarios-de-internet-en-Mexico-en-2018-20180517-0077.html

Mathiason, J. (2009). *Internet governance: the new frontier of global institutions*. London; New York: Routledge.

Mazower, M. (2014). After the crisis, nation-state strikes back. Retrieved December 2, 2014, from Gulf News Thinkers website: http://gulfnews.com/opinions/columnists/after-the-crisis-nation-state-strikes-back-1.1419157

McCullagh, D. (2009). Bill would give president emergency control of Internet. Retrieved from http://www.cnet.com/news/bill-would-give-president-emergency-control-of-internet/

McCullagh, D. (2011a). Internet "kill switch" bill will return. Retrieved January 9, 2015, from CNET website: http://www.cnet.com/news/internet-kill-switch-bill-will-return/

McCullagh, D. (2011b). Internet "kill switch" bill will return. Retrieved January 1, 2016, from CNET website: http://www.cnet.com/news/internet-kill-switch-bill-will-return/

McCullagh, D. (2011c). Renewed Push to Give Obama an Internet "Kill Switch." Retrieved March 25, 2016, from CBS News website: http://www.cbsnews.com/news/renewed-push-to-give-obama-an-internet-kill-switch/

McDonald, M. (2008). Securitization and the Construction of Security. *European Journal of International Relations*, *14*(4), 563–587. https://doi.org/10.1177/1354066108097553

McDowell, R. (2011). *Federal Communications Commission: Keynote on Technology and Democracy*. Retrieved from http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-307998A1.pdf

Medows, D. B. (2012). *The Sound of Silence: The Legality of the American "Kill Switch Bill."*

Meinrath, S. D., Losey, J. W., & Pickard, V. W. (2011). Chapter 5 - Digital Feudalism: Enclosures and Erasures from Digital Rights Management to the Digital Divide. In *Advances in Computers*: *Vol. Volume 81* (pp. 237–287). https://doi.org/10.1016/B978-0-12-385514-5.00005-7

Mejias, U. A. (2013). *Off the Network : Disrupting the Digital World.* Retrieved from https://books.google.com/books?id=Oy6uNAEACAAJ&dq=Off+the+network+:+disrupting+the+digital+world&hl=en&sa=X&ved=0ahUKEwi6hZu0kL_XAhXl6oMKHf7BAH8Q6AEIJjAA

Mennecke, T. (2010). MPA Coming After Newzbin2. Retrieved April 21, 2014, from Slyck website: http://www.slyck.com/story2144_MPA_Coming_After_Newzbin2

Merkelsson, S. (2010). Blog del Narco gets the drug war scoop. Retrieved September 29, 2015, from Foreign Policy website: http://foreignpolicy.com/2010/08/13/blog-del-narco-gets-the-drug-war-scoop/

Mesoznik, K. (2016). The Truth About Internet Freedom in Turkey. Retrieved March 23, 2017, from The Huffington Post website: http://www.huffingtonpost.com/entry/the-truth-about-internet-freedom-in-turkey_us_58389d83e4b050dfe6187ba3

Messmer, E. (2013). Rising cyber-nationalism leads to amplified cyber-mistrust. Retrieved May 2, 2017, from NetworkWorld website: http://www.networkworld.com/article/2164526/data-center/rising-cyber-nationalism-leads-to-amplified-cyber-mistrust.html

Michaelsen, M. (2016). Exit and voice in a digital age: Iran's exiled activists and the authoritarian state. *Globalizations*, 1–17. https://doi.org/10.1080/14747731.2016.1263078

Miles, M. (1994). *Qualitative data analysis : an expanded sourcebook*. Thousand Oaks: Sage Publications.

Miroff, N., & Booth, W. (2012, July 2). Peña Nieto is winner of Mexican election. *The Washington*

Post. Retrieved from http://www.washingtonpost.com/world/the_americas/mexico-presidential-election-underway/2012/07/01/gJQAyd96FW_story.html

Mitchell, B. (2017). What is a DNS cache? Retrieved May 8, 2017, from Lifeware website: https://www.lifewire.com/what-is-a-dns-cache-817514

Moncau, L. F., & Mizukami, P. N. (2014). Brazilian Chamber of Deputies Approves Marco Civil Bill » infojustice. Retrieved April 21, 2014, from infojustice website: http://infojustice.org/archives/32527

Montalvo, T. (2013). México usará información del "ciberespacio" para combatir a criminales. Retrieved March 30, 2016, from Expansion website: http://expansion.mx/nacional/2013/06/21/mexico-usara-informacion-del-ciberespacio-para-combatir-a-criminales

Moore, J. (2015). Hacker Group Anonymous Threatens Israel With "Electronic Holocaust." Retrieved October 14, 2015, from N Technology website: http://europe.newsweek.com/hacker-group-anonymous-threaten-israel-electronic-holocaust-317729

Mora, A. (2014). Actualizado: Los Andes en Emergencia y Tachira sin Internet: Estado Alma de la Lucha democratica de Venezuela. Retrieved March 11, 2014, from Apuntes de una Periodista, por Angélica Mora website: http://angelicamorabeals.blogspot.com/2014/03/en-venezuela-estado-tachira-sin-internet.html

Morlino, L. (2008). Hybrid Regimes or Regimes in Transition? In *Fundacion para las Relaciones Internacionales y el Dialogo Exterior*. Retrieved from http://www.fride.org/download/WP70-Hybrid_regimes_ENG_sep08.pdf

Morlino, L. (2009). Are there hybrid regimes? Or are they just an optical illusion? *European Political Science Review*, *1*(2), 273–296. Retrieved from http://studium.unict.it/dokeos/2011/courses/1001283C0/document/morlinoEPSR2009.pdf

Morozov, E. (2011). How the Kremlin Harnesses the Internet - NYTimes.com. Retrieved April 21, 2014, from The New York Times website: http://www.nytimes.com/2011/01/05/opinion/05iht-edmorozov04.html

MrBarbacoa2011. (2010). *Hugo Chavez va por el internet "'no puede ser una cosa libre.'"* Retrieved from https://www.youtube.com/watch?v=SU49tNOBK98

Mueller, M. (2002). *Ruling the root Internet governance and the taming of cyberspace*. Cambridge, Mass. : MIT Press,.

Mueller, M. (2010). A Battle for the Soul of the Internet. In *Networks and States* (pp. 1–13). Cambridge, Massachusetts: MIT Press.

Mueller, M. (2010). *Networks and States: the Global Politics of Internet Governance*. Cambridge Mass.: MIT Press.

Muggah, R. (2013). After NSA scandal, will Brazil try to unravel the Internet? Retrieved June 24, 2015, from The Globe and Mail website: http://www.theglobeandmail.com/globe-debate/after-nsa-scandal-will-brazil-try-to-unravel-the-internet/article14407678/

Murray, A. (2003). Regulation and Rights in Networked Space. *Journal of Law and Society*, *30*(2), 187–216. Retrieved from http://doi.wiley.com/10.1111/1467-6478.00253

Murray, A., Zeadally, S., & Flowers, A. (2012). An assessment of U.S. legislation on cybersecurity. *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, 289–294. https://doi.org/10.1109/CyberSec.2012.6246106

Murray, D. (2009). Freedom of Expression, Counter-Terrorism and the Internet in Light of the Uk

Terrorist Act 2006 and the Jurisprudence of the European Court of Human Rights. *Netherlands Quarterly of Human Rights*, *27*(3), 331–360.

Naim, M., & Toro, F. (2016). Venezuela Is Falling Apart -. Retrieved May 12, 2016, from The Atlantic website: http://www.theatlantic.com/international/archive/2016/05/venezuela-is-falling-apart/481755/?utm_source=atltw

Nakashima, E. (2016). Obama administration is close to announcing measures to punish Russia for election interference. Retrieved September 20, 2017, from The Washington Post website: https://www.washingtonpost.com/world/national-security/the-white-house-is-scrambling-for-a-way-to-punish-russian-hackers-via-sanctions/2016/12/27/0eee2fdc-c58f-11e6-85b5-76616a33048d_story.html?utm_term=.b5d24ab2fc62

NDTV. (2011). Cameron exploring crackdown on social media after riots. Retrieved August 17, 2017, from NDTV website: http://www.ndtv.com/world-news/cameron-exploring-crackdown-on-social-media-after-riots-464418

Netnod. (2014). what is an internet exchange point? Retrieved February 6, 2018, from NETNOD Fact Sheet website: https://www.netnod.se/sites/default/files/ix/Materials/what_is_an_ixp_Netnod_fact_sheet.pdf

Netnod. (2018). What is peering. Retrieved February 27, 2018, from NETNOD website: https://www.netnod.se/ix/what-is-peering

Neuman, W. (2013, April 16). Post-Election Tensions Rise in Venezuela Amid Deadly Protests - The New York Times. *The New York Times*. Retrieved from http://www.nytimes.com/2013/04/17/world/americas/post-election-tensions-rise-in-venezuela-amid-deadly-protests.html

Niedrich, A. N. (2011). Emphasizing Substance: Making the Case for a Shift in Political Speech Jurisprudence. *University of Michigan Journal of Law Reform*, *44*(4). Retrieved from http://repository.law.umich.edu/mjlr

Nikkarila, J.-P., & Ristolainen, M. (2017). 'RuNet 2020' - deploying traditional elements of combat power in cyberspace? *2017 International Conference on Military Communications and Information Systems (ICMCIS)*, 1–8. https://doi.org/10.1109/ICMCIS.2017.7956478

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, *91*(1), 111–130. https://doi.org/10.1111/1468-2346.12189

Norton, W. B. (2001). *Internet Service Providers and Peering*. Retrieved from https://www.cs.rutgers.edu/~badri/552dir/papers/bgp/norton-peering.pdf

Norton, W. B. (2014). What is an Internet Exchange Point? Retrieved February 23, 2014, from DrPeering website: http://drpeering.net/FAQ/What-is-an-Internet-Exchange-Point.php

Norzagaray Lopez, M. D. (2008). *El narcotrafico en Mexico desde el discurso oficial [Drug trafficking in Mexico: the official speech]*. Retrieved from http://www.flacso.edu.mx/biblioiberoamericana/TEXT/MCS_XVII_promocion_2008-2010/Norzagaray_MD.pdf

Nosowitz, D. (2011). U.K. Prime Minister David Cameron Wants a Master Kill-Switch for Social Networks | Popular Science. Retrieved July 21, 2014, from Popular Science website: http://www.popsci.com/technology/article/2011-08/uk-prime-minister-david-cameron-considers-switching-entire-social-networks

noticias24. (2013). Arreaza informó que hubo "45 mil intentos de hackeo desde el exterior" a la página del CNE [Arreaza informed that there were "45 thousand attempts to hack from abroad" to the CNE webpage]. Retrieved October 26, 2015, from Noticias 24 Venezuela

website: http://www.noticias24.com/venezuela/noticia/162656/arreaza-informa-que-no-hay-problemas-con-internet-fue-una-maniobra-para-impedir-mas-hackeos/

noticias24. (2014). Gobierno bloqueó “varios de los enlaces” de Internet “desde donde se atacan sitios públicos.” Retrieved October 26, 2015, from Noticias 24 Venezuela website: http://www.noticias24.com/venezuela/noticia/222213/gobierno-bloqueo-varios-de-los-enlaces-de-internet-desde-donde-se-atacan-sitios-publicos/

Noticias24. (2014). Restituyen servicio de internet Banda Ancha en el Táchira tras hechos violentos. Retrieved July 18, 2017, from Noticias24 website: http://www.noticias24.com/venezuela/noticia/223671/restituyen-servicio-de-internet-banda-ancha-en-el-tachira-tras-hechos-violentos/

NSTAC. (2006). Termination of Cellular Networks During Emergency Situations. *NSTAC Issue Review*, 139–140. Retrieved from https://s3.amazonaws.com/s3.documentcloud.org/documents/686341/sop-303.pdf

Nuñez, E., & Ochoa, A. (2013). Venezuela: Nicolás Maduro gana por estrecha diferencia [Venezuela: Nicolás Maduro wins by narrow gap]. Retrieved March 15, 2017, from BBC Mundo - Noticias website: http://www.bbc.com/mundo/noticias/130412_livetext_venezuela_elecciones_presidenciales_ao.shtml

Nye, J., & Donahue, J. (2000). *Governance in a globalizing world*. Cambridge, Mass. :;Washington, D.C. : Visions of Governance for the 21st Century ;;Brookings Institution Press,.

O’Neill, P. H. (2016). Russia lawmakers pass sweeping spying law that requires encryption backdoors, call surveillance. Retrieved March 15, 2017, from The Daily Dot website: https://www.dailydot.com/layer8/encryption-backdoor-russia-fsb-bill-passes/

Obrien, D. (2014). Venezuela’s Internet Crackdown Escalates into Regional Blackout. Retrieved March 4, 2014, from EFE - Electronic Frontier Foundation website: https://www.eff.org/deeplinks/2014/02/venezuelas-net-crackdown-escalates

OECD. (2014). List of OECD Member countries - Ratification of the Convention on the OECD. Retrieved April 21, 2014, from Better Policies for Better Lives website: http://www.oecd.org/about/membersandpartners/list-oecd-member-countries.htm

Ogundeji, O. (2017). Internet shutdown in Cameroon continues -. Retrieved February 12, 2017, from ITWeb Africa website: http://www.itwebafrica.com/network/479-cameroon/237396-internet-shutdown-in-cameroon-continues

Oi, M. (2014). Turkey moves to block YouTube access after “audio leak.” Retrieved March 29, 2014, from BBC website: http://www.bbc.com/news/world-europe-26773702

Oleg, D., Kulikova, A., Lukatsky, A., Makarova, O., & Kolesnikov, A. (2017). Global Internet Governance and Cyber Security: As Viewed by Russian Experts. *PIR Center*. Retrieved from http://pircenter.org/en/news/6921-pir-center-library-presents-new-collection-of-articles-global-internet-governance-and-cyber-security-as-viewed-by-russian-experts

Olukotun, D., & Pallero, J. (2016). Brazil moves to block WhatsApp (again). Retrieved October 2, 2016, from Access Now website: https://www.accessnow.org/brazil-moves-block-whatsapp/

ONG Derechos Digitales, APC, & Varon Ferraz, J. (2014). *Latin America in a Glimpse: Human Rights and the Internet*. Santiago de Chile.

ONI. (2014). About Filtering. Retrieved March 20, 2017, from OpenNet Initiative website: https://opennet.net/about-filtering

Opderbeck, D. W. (2012). Cybersecurity and Executive Power. *Washington University Law Review*, Vol. 89, pp. 795–845. Retrieved from http://openscholarship.wustl.edu/law_lawreview/vol89/iss4/2

Opderbeck, D. W. (2013). Does the Communications Act of 1934 Contain a Hidden Internet Kill Switch? *Federal Communications Law Journal*, *65*(1). Retrieved from http://www.fclj.org/wp-content/uploads/2013/01/65-1-operdeck.pdf

OpenNet. (2006). Nepal. Retrieved February 8, 2014, from https://opennet.net/sites/opennet.net/files/nepal.pdf

OpenNet. (2013). OpenNet Initiative. Retrieved from OpenNet Initiative website: https://opennet.net/

OpenNet Initiative. (2005). Nepal: Internet Down, Media Censorship Imposed. Retrieved February 12, 2018, from OpenNet Initiative website: https://opennet.net/blog/2005/02/nepal-internet-down-media-censorship-imposed

Oppenheimer, A. (2015, November 13). ¡Se Despertó la OEA! [The OAS Woke Up]. *El Mundo*. Retrieved from http://www.elmundo.es/internacional/2015/11/13/564464b446163f52598b460e.html

Oppermann, D. (2014). Internet Governance and Cybersecurity in Brazil. In *Multilateral Security Governance, Conference of Forte de Copacabana* (pp. 167–181). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2587178

Ore, D., & Chinea, E. (2017). Maduro convoca Asamblea Constituyente en Venezuela, oposición llama a rebelarse [Maduro Convokes Constituent Assembly in Venezuela, Opposition calls to rebellion]. Retrieved March 12, 2018, from Reuters website: https://lta.reuters.com/article/domesticNews/idLTAKBN17X1VJ-OUSLD?sp=true

OSCE RFOM. (2009). *Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship*. Retrieved from https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/speak_up/osce_freedom_of_the_media_on_turkey_and_internet_censorship.pdf

Pahwa, N. (2015). On Internet bans in India and the "Internet kill switch." Retrieved April 19, 2016, from MediaNama website: http://www.medianama.com/2015/09/223-internet-bans-india/

Pahwa, N. (2016). Derek O ' Brien on Internet shutdowns in Kashmir ; Our take. Retrieved August 11, 2016, from MEDIANAMA website: http://www.medianama.com/2016/08/223-derek-obrien-internet-shutdowns-kashmir-take/

Paleri. (2008). *National Security: Imperatives and Challenges*. Retrieved from http://books.google.com/books?id=DMzcGe0-HQwC&pgis=1

Pallero, J. (2016). Cybercrime proposals would gut digital rights in Brazil. Act now. Retrieved from Aces Now website: https://www.accessnow.org/stop-cybercrime-reforms-cpiciber-brazil/

Pallero, J., & Olukotun, D. (2015). Access Now condemns blocking of WhatsApp in Brazil - Access Now. Retrieved January 28, 2016, from accessnow website: https://www.accessnow.org/access-now-condemns-blocking-whatsapp-brazil/

Papacharissi, Z., & de Fatima Oliveira, M. (2012). Affective News and Networked Publics: The Rhythms of News Storytelling on #Egypt. *Journal of Communication*, *62*(2), 266–282. https://doi.org/10.1111/j.1460-2466.2012.01630.x

Pardo, D. (2016). 5 estampas de cómo se ha deteriorado la vida en Venezuela. Retrieved February 26, 2017, from BBC MUNDO website:

http://www.bbc.com/mundo/noticias/2016/04/160428_venezuela_calidad_de_vida_dp
PCH. (2015). Packet Clearing House Report on Internet Exchange Point Locations. Retrieved March 7, 2014, from PCH website: https://prefix.pch.net/applications/ixpdir/summary/
PCH. (2017). Internet Exchange Directory. Retrieved March 19, 2017, from Packet Clearing House website: https://www.pch.net/ixp/dir
Peralta, E. (2014). Brazil Becomes One Of The First To Adopt Internet 'Bill Of Rights' : The Two-Way : NPR. Retrieved July 2, 2015, from the two-way website: http://www.npr.org/sections/thetwo-way/2014/04/23/306238622/brazil-becomes-one-of-the-first-to-adopt-internet-bill-of-rights
Perfil Internacional. (2010). Hugo Chávez: "Internet no puede ser libre." Retrieved November 18, 2015, from Perfil Internacional website: http://www.perfil.com/internacional/Hugo-Chavez-Internet-no-puede-ser-libre-20100316-0004.html
Perlroth, N., & Sanger, D. E. (2014, December 22). North Korea Loses Its Link to the Internet. *The New York Times*. Retrieved from https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html
PESTLE. (2015a). Political Factors Affecting Business. Retrieved March 12, 2017, from PESTLE ANALYSIS website: http://pestleanalysis.com/political-factors-affecting-business/
PESTLE. (2015b). What is Environmental Analysis? Retrieved March 12, 2017, from PESTLE ANALYSIS website: http://pestleanalysis.com/what-is-environmental-analysis/
PESTLE. (2017). What is PESTLE Analysis? A Tool for Business Analysis. Retrieved March 12, 2017, from PESTLE ANALYSIS website: http://pestleanalysis.com/what-is-pestle-analysis/
Peterson, A. (2014). The Sony Pictures hack, explained. Retrieved October 10, 2018, from The Washington Post website: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?noredirect=on&utm_term=.a87072f914df
POST. (2011). Cyber Security in the UK. *Houses of Parliament*, Vol. 389. Retrieved from http://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-uk.pdf
POST. (2017). Cyber Security of UK Infrastructure. Retrieved August 30, 2017, from Houses of Parliament. Parliamentary Office of Science & Technology website: http://researchbriefings.files.parliament.uk/documents/POST-PN-0554/POST-PN-0554.pdf
Postel, J. (1980). *DoD standard Internet Protocol*. https://doi.org/Defense Advanced Research Projects Agency Information Processing Techniques Office
Postel, J. (1981). *Internet Protocol*. Retrieved from https://tools.ietf.org/html/rfc791
Poznanski, F., Internet Without Borders, Blanc, F., Valente, J., & Vicentin, D. (2017). IGF 2017 WS #128 The future of Internet governance: submarine cables and global inter-connectivity | Internet Governance Forum. Retrieved September 9, 2018, from Internet Governance Forum - IGF website: https://www.intgovforum.org/multilingual/content/igf-2017-ws-128-the-future-of-internet-governance-submarine-cables-and-global-inter
Price, R. (2015). David Cameron's proposed encryption ban would "destroy the internet." Retrieved July 16, 2015, from Business Insider Australia website: http://www.businessinsider.com.au/bruce-schneier-david-cameron-proposed-encryption-ban-destroy-the-internet-2015-7?r=U
Prigg, M. (2013). Web inventor Sir Tim Berners-Lee denies "off-switch" for the internet | Mail Online. Retrieved August 28, 2013, from Science and Tech - Mail Online website: http://www.dailymail.co.uk/sciencetech/article-2198668/Web-inventor-Sir-Tim-Berners-

Lee-denies-switch-internet.html
Pynnöniemi, K. (2012a). *Critical infrastructure protection: an evolution of Russian policy*. Retrieved from http://www.fiia.fi/assets/events/Presentation_KP_18_12_poist.pdf
Pynnöniemi, K. (2012b). *Russian critical infrastructures*. Retrieved from https://www.files.ethz.ch/isn/157058/FIIAReport35_web.pdf
Pynnöniemi, K. (2012c). The evolution of Russian policy on critical infrastructure protection. In K. Pynnöniemi (Ed.), *Russian Critical Infrastructures*. Retrieved from http://www.fiia.fi/assets/publications/FIIAReport35_web.pdf
Radvanovsky, R. (2006). *Critical Infrastructure* (1st ed.). Retrieved from http://www.crcnetbase.com.libezproxy2.syr.edu/doi/book/10.1201/9781420007428
Radvanovsky, R., & McDougall, A. (2009). *Critical Infrastructure* (2ND.). Retrieved from http://www.crcnetbase.com/doi/book/10.1201/9781420095289
Ramos, D. (2014). Bloqueo, censura... ¿Qué propone Peña Nieto para internet? Retrieved October 22, 2014, from Animal Político website: http://www.animalpolitico.com/2014/03/bloqueo-de-senal-censura-que-propone-pena-nieto-para-internet/
RAND. (2017). Cyber Warfare. Retrieved August 25, 2018, from RAND website: https://www.rand.org/topics/cyber-warfare.html
Rawlinson, K. (2014). Turkey blocks use of Twitter after prime minister attacks social media site. Retrieved September 21, 2015, from The Guardian website: http://www.theguardian.com/world/2014/mar/21/turkey-blocks-twitter-prime-minister
Reichert, C. (2015). Telco national security draft legislation released, again. Retrieved November 11, 2017, from ZDNet website: http://www.zdnet.com/article/telco-national-security-draft-legislation-released-again/
Reitinger, P., Butler, R. J., Schwartz, A., & Chipman, J. (2011). Statement for the Record of Philip Reitinger, Deputy Under Secretary, National Protection and Programs Directorate, before the Senate Homeland Security and Governmental Affairs Committee: "Protecting Cyberspace: Assessing the White House Proposal." Retrieved September 30, 2014, from Official website of the Department of Homeland Security website: https://www.dhs.gov/news/2011/05/23/statement-record-philip-reitinger-deputy-under-secretary-national-protection-and
Reitinger, P., Butler, R., Schwartz, A., & Chipman, J. (2011). *Statement for the Record*. Retrieved from http://www.justice.gov/ola/testimony/112-1/05-23-11-odag-chipman-testimony-re-protecting-cyberspace---assessing-the-white-house-proposal.pdf
Reuters. (2007, January 10). YouTube Is Back Online in Brazil. *New York Times*. Retrieved from http://www.nytimes.com/2007/01/10/business/worldbusiness/10youtube.html
Reuters. (2013). U.S. Homeland Chief: Cyber 9/11 could happen imminently. Retrieved March 4, 2018, from Reuters website: https://www.reuters.com/article/us-usa-cyber-threat/u-s-homeland-chief-cyber-9-11-could-happen-imminently-idUSBRE90N1A320130124
Reuters. (2014, December 12). Google Pulling Engineers Out of Russia Amid Tightening Control, Report Says. *The Moscow Times*. Retrieved from http://www.themoscowtimes.com/business/article/google-pulling-engineers-out-of-russia-amid-tightening-control-report-says/513237.html
Reuters. (2015, October 6). Russia Says Google Must Correct Mobile Contracts by Nov. 18. *The Moscow Times*. Retrieved from http://www.themoscowtimes.com/business/article/russia-says-google-must-correct-mobile-contracts-by-nov-18/537245.html
Reuters. (2017a). LinkedIn fails to agree with Russia on restoring access to site. Retrieved

September 20, 2017, from REUTERS website: http://www.reuters.com/article/us-linkedin-russia-ban/linkedin-fails-to-agree-with-russia-on-restoring-access-to-site-idUSKBN16E20Q

Reuters. (2017b). Venezuela Pulls CNN From Airwaves for "Distorting Truth." Retrieved March 15, 2017, from Newsweek website: http://www.newsweek.com/venezuela-censorship-nicolas-maduro-cnn-censorship-557305

RIA Novosti. (2014). Russian Lawmaker Proposes Domestic Internet. Retrieved March 15, 2017, from Sputnik website: https://sputniknews.com/russia/20140428189429763-Russian-Lawmaker-Proposes-Domestic-Internet/

Richards, J. (2012). *A guide to national security : threats, responses and strategies*. Oxford ;;New York: Oxford University Press.

Ridley, D. (2008). *The literature review : a step-by-step guide for students*. Retrieved from http://www.worldcat.org/title/literature-review-a-step-by-step-guide-for-students/oclc/181069250&referer=brief_results

Riley, C. (2017). Russia bans VPNs to stop users from looking at censored sites - Jul. 31, 2017. Retrieved August 1, 2017, from CNN Tech website: http://money.cnn.com/2017/07/31/technology/russia-vpn-internet-putin/index.html

Robinson, G. (2009, September 3). Nation's web access cut after Telstra outage. *The Sydney Morning Herald*. Retrieved from http://www.smh.com.au/technology/technology-news/nations-web-access-cut-after-telstra-outage-20090902-f8uz

Rose, M. T. (1990). Transition and Coexistence Strategies for TCP/IP to OSI. *IEEE Xplore*, *8*(1), 57–66. Retrieved from https://ieeexplore.ieee.org/abstract/document/46846/authors#authors

Rosenne, S., & Hague Academy of International Law. (2004). *The Perplexities of Modern International Law*. Leiden; Boston: Martinus Nijhoff.

Rossini, C., Cruz, F. B., & Doneda, D. (2015). *The Strengths and Weaknesses of the Brazilian Internet Bill of Rights: Examining a Human Rights Framework for the Internet*. Retrieved from https://www.cigionline.org/sites/default/files/no19_0.pdf

Rothe, D. (2015). *Securitizing Global Warming: A Climate of Complexity*. Retrieved from https://books.google.com/books?id=0IP4CgAAQBAJ&pg=PA16&lpg=PA16&dq="Security+as+Speech+Act"&source=bl&ots=EnrWxD5_NS&sig=aIo0b6g6DlMVu2Man5w0fsNavHw&hl=en&sa=X&ved=0ahUKEwj4kfWo7pnSAhUn0oMKHULpD9kQ6AEIKDAC#v=onepage&q="Security a

Rouseff, D. (2013). *Statement by H.E. Dilma Rousseff, President of the Federative Republic of Brazil*. Retrieved from http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf

Rozell, M. J., & Sollenberger, M. A. (2013). The Unitary Executive Theory and the Bush Legacy. In D. R. Kelley & T. G. Shields (Eds.), *Taking the Measure: The Presidency of George W. Bush* (pp. 36–54). Retrieved from http://markrozell.gmu.edu/wp-content/uploads/2011/11/Rozell_and_Sollenberger_UE_and_Bush_Legacy_Chapter_2013.pdf

Rozell, M. J., & Sollenberger, M. A. (2015). Presidents: Executive Privilege. In D. A. Bearfield, E. M. Berman, & M. J. Dubnick (Eds.), *Encyclopedia of Public Administration and Public Policy* (3rd ed., pp. 1–5). https://doi.org/10.1081/E-EPAP3-120051800

RT. (2013a). 'Erase Israel from the Internet': Anonymous plots massive cyber-attack. Retrieved October 14, 2015, from RT website: https://www.rt.com/news/anonymous-cyber-attack-israel-241/

RT. (2013b). Russia may deem civil servants' use of Gmail, Facebook 'high treason.' Retrieved January 31, 2016, from RT website: https://www.rt.com/politics/gmail-facebook-treason-

high-521/
RT. (2014a). Lawmakers seek to fast track law on personal data storage in Russia. Retrieved January 31, 2016, from RT website: https://www.rt.com/politics/184216-russia-data-law-fast/
RT. (2014b). MP urges ‘nationalization’ of Google over security fears. Retrieved January 25, 2016, from RT website: https://www.rt.com/politics/186364-russian-google-nationalization-fyodorov/
RT. (2014c). Russia won’t disconnect from global internet, works on cyber security – Kremlin. Retrieved January 31, 2016, from RT website: https://www.rt.com/news/188960-internet-blackout-russia-counter/
RT. (2014d). Russian lawmaker suspects Google of spying for Kiev regime. Retrieved June 8, 2017, from RT Russian politics website: https://www.rt.com/politics/184935-russia-ukraine-google-security/
Ruggiero, S. (2012). COMMENT: Killing the Internet to Keep America Alive: The Myths and Realities of the Internet Kill Switch.
Runkevich, D., & Malai, E. (2014). Депутаты предлагают разработать систему «автономного интернета» - Известия [MPs propose to develop a system of “autonomous Internet”]. Retrieved March 13, 2017, from «Газета Известия» ["Izvestia"] website: http://izvestia.ru/news/576191
Russell, A. (2011). The Arab Spring, Extra-National Information Flows, Social Media and the 2011 Egyptian Uprising. Retrieved September 12, 2012, from International Journal of Communication website: http://ijoc.org/ojs/index.php/ijoc/article/view/93
Russell, C. (2011). Posts about Civil Contingencies Act 2004 on Critique. Retrieved March 21, 2014, from CRITique website: https://charlesrussell.wordpress.com/tag/civil-contingencies-act-2004/
Russia Beyond the Headlines. (2015, November 12). Expert says immediate Runet shutdown impossible. *Russia Beyond the Headlines*. Retrieved from http://rbth.com/news/2014/11/12/expert_says_immediate_runet_shutdown_impossible_41329.html
Rydzak, J. (2017). Digilantes: The Determinants of Internet and Cell Phone Shutdowns in War and Peace. *ISA Annual Convention, Baltimore, 2017*. Retrieved from http://web.isanet.org/Web/Conferences/Baltimore 2017-s/Archive/a0ac7e09-f21d-43ac-bd99-3fb67cc16690.pdf
Ryter, J. C. (2009). Australia tests 24-hour takeover of Aussieland ISPs as Democrats try to regulate the Internet at home. Retrieved April 29, 2014, from Jon Christian Ryter’s Conservative World website: http://www.jonchristianryter.com/Two_Cents/2cworth.090919.html
Sainsbury, M. (2009). Telstra enters NBN race. Retrieved March 19, 2017, from news.com.au website: http://www.news.com.au/news/telstra-enters-nbn-race/news-story/6c1c46b912438551ba81926250889265
Sanger, D. E. ., & Schmitt, E. (2015, October 25). Russian Ships Near Data Cables Are Too Close for U.S. Comfort. *The New York Times*. Retrieved from http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html
Schmidt, H. (2011). The Administration Unveils its Cybersecurity Legislative Proposal. Retrieved September 25, 2013, from THe White House Blog website:

http://www.whitehouse.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal

Schneidewind, N. (2010). Metrics for Mitigating Cybersecurity Threats to Networks. *IEEE Internet Computing*, *14*(1), 64–71. https://doi.org/10.1109/MIC.2010.14

Schneier, B. (1996). *Applied cryptography : protocols, algorithms, and source code in C*. New York: Wiley.

Seals, T. (2018). Cyber-attack Volume Doubled in First Half of 2017. Retrieved January 28, 2018, from Infosecurity Magazine website: https://www.infosecurity-magazine.com/news/cyberattack-volume-doubled-2017

Segal, A. (2017). Brazil's Internet Is Under Attack, Again. Retrieved August 18, 2017, from Council on Foreign Relations website: https://www.cfr.org/blog/brazils-internet-under-attack-again

Sen Lieberman, J. I. (2010, June 10). S.3480 Titles. Retrieved September 14, 2013, from http://thomas.loc.gov/cgi-bin/bdquery/z?d111:SN03480:@@@T

Sen Lieberman, J. I. (2011, February 17). *S.413 - Cybersecurity and Internet Freedom Act of 2011*. Retrieved from http://thomas.loc.gov/cgi-bin/bdquery/z?d112:s.413:

Senator Carper. (2011). Press Releases - Tom Carper, U.S. Senator for Delaware. Retrieved January 31, 2016, from Tom Carper U.S. Senator for Delaware website: http://www.carper.senate.gov/public/index.cfm/pressreleases?ID=0b2905fc-6f60-450a-9bd7-ac8a3b6ab341

Senator Collins. (2011). *Statement on Introduction of Cyber Security and Internet Freedom Act of 2011*. Retrieved from http://politechbot.com/docs/collins.cybersecurity.bill.floor.021711.txt

Senator Lieberman. (2010). *S. 3480, The Protecting Cyberspace as a National Asset Act*. Retrieved from http://www.hsgac.senate.gov/download/2010-06-24-lieberman-statement

Senator Lieberman. *Actions - S.413 - 112th Congress (2011-2012): Cybersecurity and Internet Freedom Act of 2011*. , (2011).

Senator Lieberman. *Text Original - S.413 - 112th Congress (2011-2012): Cybersecurity and Internet Freedom Act of 2011*. , (2011).

Senator Rockefeller. *Actions - S.773 - 111th Congress (2009-2010): Cybersecurity Act of 2010*. , (2010).

Senator Stephen Conroy. (2008). *Towards a framework for cybersecurity and critical information infrastructure protection. Address to ITU Cybersecurity Forum*. Retrieved from https://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/conroy-ministerial-address-brisbane-july-08.pdf

Shane, P. (2012). Cybersecurity: Toward a Meaningful Policy Framework. Retrieved February 3, 2014, from Texas Law Review website: https://www.academia.edu/3623387/Cybersecurity_Toward_a_Meaningful_Policy_Framework_90_Texas_Law_Review_See_Also_87_2012_

Shane, P. M. (2012). *Cybersecurity: Toward a Meaningful Policy Framework*. Retrieved from http://papers.ssrn.com/abstract=2284279

Shin, J. (2015). The FOIA Fight for SOP 303. Retrieved March 6, 2018, from Fordham Intellectual Property, Media & Entertainment Law Journal website: http://www.fordhamiplj.org/2015/11/15/the-foia-fight-for-sop-303/

Shirky, C. (2011). The political power of social media: Technology, the public sphere, and political change. *Foreign Affairs*, *90*(1), 28–41.

Sifir, C. (2014). How did the Turkish government seal off and block people from Twitter?

Retrieved September 21, 2015, from Quora website: https://www.quora.com/How-did-the-Turkish-government-seal-off-and-block-people-from-Twitter

Singel, R. (2009). Australia Censors Wikileaks Page. Retrieved April 21, 2014, from WIRED website: http://www.wired.com/2009/03/australia-censo

Slapper, G., & Kelly, D. (2008). *The English Legal System* (9th ed.). London; New York: Routledge-Cavendish.

Slim, R. (2016). Can Anyone Stop the Syrian War? Retrieved December 16, 2016, from Foreign Policy website: http://foreignpolicy.com/2016/09/12/can-anyone-stop-the-syrian-war-us-russia-ceasefire-spoilers/

Sorensen, K. (1996). Silencing the Net: The Threat to Freedom of Expression On-line. Retrieved November 4, 2017, from Human Rights Watch website: https://epic.org/free_speech/intl/hrw_report_5_96.html

SOSVenezuela2014. (2014). *Ministro Manuel Fernández 24-02-2014*. Retrieved from https://www.youtube.com/watch?v=s2rQxPX5SFU

Springer, P. J. (2017). *Encyclopedia of cyber warfare*. Retrieved from https://books.google.com/books?id=9tgoDwAAQBAJ&pg=PA325&lpg=PA325&dq="From+now+on,+our+digital+infrastructure+–+the+networks+and+computers+we+depend+on+every+day+–+will+be+treated+as+they+should+be:+as+a+strategic+national+asset.++Protecting+this+infrastr

Stack, L. (2011a). Activists Using Video to Bear Witness in Syria. *New York Times*. Retrieved from http://www.nytimes.com/2011/06/19/world/middleeast/19syria.html?sq=Liam Stack Syria&st=cse&adxnnl=1&scp=3&adxnnlx=1394568541-QLjsuCwmCldygV3GHdRuig

Stack, L. (2011b). Mourning a Boy, Crowds in Syria Defy Crackdown . *New York Times (Late New York Edition)*, A1, A8. Retrieved from http://vnweb.hwwilsonweb.com.libezproxy2.syr.edu/hww/jumpstart.jhtml?recid=0bc05f7a67b1790e9e8f8b7ba40311062afa1d6bf4c1018599f546d44e60ea31db553378953c8f84&fmt=C

Stiles, J. (2016). Bad start to long weekend for Telstra customers. Retrieved June 13, 2016, from New Daily website: http://thenewdaily.com.au/life/2016/06/11/telstra-internet-outage/

Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. *International Affairs Journal of Cyber Policy*, *92*(5). Retrieved from https://www.chathamhouse.org/publication/ia/uk-cyber-security-and-critical-national-infrastructure-protection

Stone, J. (2014a). Kremlin Mulls Internet "Kill Switch" To Knock Russia Offline During Emergencies. *International Bussiness Times*. Retrieved from http://www.ibtimes.com/kremlin-mulls-internet-kill-switch-knock-russia-offline-during-emergencies-1693840

Stone, J. (2014b). Russia Investigating Better Cybersecurity, Not Internet "Kill Switch," Putin Says. Retrieved September 1, 2015, from International Business Times website: http://www.ibtimes.com/russia-investigating-better-cybersecurity-not-internet-kill-switch-putin-says-1697775

Streitfeld, D. (2013). Keeping the Internet Safe From Governments. *Bits - The New York Times*. Retrieved from http://bits.blogs.nytimes.com/2013/01/23/keeping-the-internet-free/?_r=1

Subcommittee on Cybersecurity. (2011). *Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies*. Retrieved from

http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg74646/pdf/CHRG-112hhrg74646.pdf
Subramanian, R. (2011). The Growth of Global Internet Censorship and Circumvention: A Survey. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2032098
Suleyman, C. (2017). A moment that changed me: walking home through the London riots in 2011 | Chimene Suleyman. Retrieved August 8, 2017, from theguardian2 website: https://www.theguardian.com/commentisfree/2017/aug/04/a-moment-that-changed-me-london-riots-2011
Sullivan, B. (2016). Could a Russian Ship Be Messing With Syria's Underwater Internet Cables? - Motherboard. Retrieved July 30, 2017, from Motherboard website: https://motherboard.vice.com/en_us/article/qkjxk5/this-theory-about-a-russian-ship-tapping-syrian-internet-is-weird
Taylor, A. (2011). Riots in London. Retrieved August 8, 2017, from The Atlantic website: https://www.theatlantic.com/photo/2011/08/riots-in-london/100124/
Taylor, A. (2016, June 29). Russia could disconnect itself from global Internet during a crisis, Putin adviser says. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2016/12/29/russia-could-disconnect-itself-from-global-internet-during-a-crisis-putin-adviser-says/?utm_term=.7d6e7e07142d
Taylor, J. (2012). How did Dodo break the internet? Retrieved August 11, 2017, from ZDNet website: http://www.zdnet.com/article/how-did-dodo-break-the-internet/
Tellis, W. (1997). Application of a Case Study Methodology. *The Qualitative Report*, *3*(3), 1–17. Retrieved from http://www.nova.edu/ssss/QR/QR3-3/tellis2.html
Terra. (2014). ¿En qué consiste la Reforma en Telecomunicaciones 2014 de Peña Nieto? Retrieved October 2, 2015, from terra website: http://noticias.terra.com.mx/mexico/politica/en-que-consiste-la-ley-de-telecom-impulsada-por-pena-nieto,8ee6d7ac1a685410VgnVCM10000098cceb0aRCRD.html
The Catalist. (2010). Mexico 2050: The World´s Fifth Largest Economy. Retrieved April 21, 2014, from TheCatalist website: http://thecatalist.org/2010/03/mexico-2050-the-world´s-fifth-largest-economy/
The Churchill Society. (1939). The Russian Enigma. BBC Broadcast 1st October 1939. Retrieved October 23, 2018, from The Churchill Society. London. website: http://www.churchill-society-london.org.uk/RusnEnig.html
The Economist. (2007). A walk on the dark side. Retrieved August 2, 2017, from The Economist website: http://www.economist.com/node/9723768
The Moscow Times. (2016). Presidential Adviser Says Russia Could Be Cut Off From Internet. Retrieved September 20, 2017, from The Moscow Times website: https://themoscowtimes.com/news/presidential-adviser-russia-could-be-cut-off-from-internet-56693
The Moscow Times. (2017, August 18). After Media Law, Foreign Ownership of Russian Internet Operators Could Be Next. *The Moscow Times*. Retrieved from https://themoscowtimes.com/news/after-media-law-further-foreign-ownership-restrictions-58696
The Moscow Times. (2018). Russia Is Ready for a Shut-Down of the Internet — Putin's Adviser. Retrieved March 17, 2018, from The Moscow Times website: https://themoscowtimes.com/news/russia-is-ready-for-a-shut-down-of-the-internet-putins-adviser-60704

The Washington Post, & Reuters. (2016). Russia moves to block LinkedIn. Retrieved September 20, 2017, from The Washington Post website: https://www.washingtonpost.com/video/business/technology/russia-moves-to-block-linkedin/2016/11/17/7005a16a-ad0c-11e6-8f19-21a1c65d2043_video.html?utm_term=.c6484df3c937

theguardian. (2017). Venezuelan opposition leader's sentence upheld day after Trump calls for release. Retrieved March 6, 2017, from theguardian website: https://www.theguardian.com/world/2017/feb/16/venezuelan-opposition-leaders-14-year-sentence-upheld

Theohary, C. A., & Rollins, J. (2011). *CRS Report for Congress Terrorist Use of the Internet: Information Operations in Cyberspace*. Retrieved from https://fas.org/sgp/crs/terror/R41674.pdf

Thomas, G. (2011). A Typology for the Case Study in Social Science Following a Review of Definition, Discourse, and Structure. *Qualitative Inquiry*, *17*(6), 511–521. https://doi.org/10.1177/1077800411409884

Thompson, K. (2012). Not like an Egyptian: Cybersecurity and the internet kill switch debate. *Texas Law Review*, *90*(2), 465–495.

Timmons, H. (2015). The BRICs era is over, even at Goldman Sachs. Retrieved January 27, 2018, from Quartz website: https://qz.com/544410/the-brics-era-is-over-even-at-goldman-sachs/

Toor, A. (2016). Bahrain's internet shutdown marks a "new form of information control." Retrieved August 4, 2016, from The Verge website: http://www.theverge.com/2016/8/4/12373676/bahrain-internet-shutdown-duraz-protests

Torzillo, J., & Scott, L. (2010). Designing with E-Stop Switches. Retrieved March 11, 2014, from machine design website: http://machinedesign.com/archive/designing-e-stop-switches

Treisman, D. (2016, April 18). Why Putin Took Crimea. Retrieved March 17, 2018, from Foreign Affairs website: https://www.foreignaffairs.com/articles/ukraine/2016-04-18/why-putin-took-crimea

trend. (2014). Turkey's general assembly ratifies Internet bill. Retrieved December 28, 2014, from trend news agency website: http://www.aa.com.tr/en/s/293504--turkey-s-general-assembly-ratifies-internet-bill

Trump, D. J. (2017). *Donald Trump Tweet*. Retrieved from https://twitter.com/realDonaldTrump/status/908643633901039617

Tsvetkova, M., & Osborn, A. (2016). Russia starts blocking LinkedIn website after court ruling. Retrieved September 20, 2017, from REUTERS website: http://www.reuters.com/article/us-russia-linkedin/russia-starts-blocking-linkedin-website-after-court-ruling-idUSKBN13C0RN

Tufekci, Z., & Wilson, C. (2012). Social Media and the Decision to Participate in Political Protest: Observations From Tahrir Square. *Journal of Communication*, *62*(2), 363–379. https://doi.org/10.1111/j.1460-2466.2012.01629.x

tutorialspoint. (2019). IPv4 Packet Structure. Retrieved March 20, 2019, from tutorialspoint website: https://www.tutorialspoint.com/ipv4/ipv4_packet_structure.htm

Tuutti, C. (2011, February 3). Minister: No Internet "Kill Switch" for Australia. *ExecutiveBiz*. Retrieved from http://blog.executivebiz.com/2011/02/minister-no-internet-kill-switch-for-australia/

U.S. Congress. *Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorist (USA Patriot Act) Act of 2001*. , (2001).

U.S. Senate. (2010a). Committee Reports - 111th Congress (2009-2010) - Senate Report 111-384.

U.S. Senate. (2010b). Committee Reports 111th Congress (2009-2010) Senate Report 111-368. Retrieved September 14, 2013, from THOMAS - Library of Congress website: http://thomas.loc.gov/cgi-bin/cpquery/R?cp111:FLD010:@1(sr368)

U.S. Senate. (2010c). *Introduction of the Protecting Cyberspace as a National Asset Act of 2010 (S.3480)* (pp. S4852–S4855). pp. S4852–S4855. Retrieved from http://fas.org/irp/congress/2010_cr/s3480.html

U.S. Senate. (2010d). S. Rept. 111-368 - Protecting Cyberspace as a National Asset Act of 2010. In *Congress Gov - Library of Congress*. Retrieved from https://www.congress.gov/congressional-report/111th-congress/senate-report/368

U.S. Senate. (2010e). *Senate Report 111-384 - CYBERSECURITY ACT OF 2010*. Retrieved from https://www.congress.gov/congressional-report/111th-congress/senate-report/384

U.S. Senate, Sumit Ghosh; Elliot Turrini, Sen Rockefeller, John D., I., Rockefeller, J., Nimmo, K., McCullagh, D., & CDT. (2010). Cybersecurity Act Of 2010 Report of the Committee on commerce, science and transportation on S.773. In *THOMAS - Library of Congress*. Retrieved from Heidelberg : Springer website: https://www.cdt.org/security/20090511_rocksnowe_analysis.pdf

Ueland, S. (2017). 20 Top Internet Service Providers. Retrieved January 21, 2019, from Practical Ecommerce website: https://www.practicalecommerce.com/20-Top-Internet-Service-Providers

Ulmer, A., & Buitrago, D. (2017). Enter the "petro": Venezuela to launch oil-backed cryptocurrency. Retrieved March 16, 2018, from REUTERS website: https://www.reuters.com/article/us-venezuela-economy/enter-the-petro-venezuela-to-launch-oil-backed-cryptocurrency-idUSKBN1DX0SQ

UN. (2014a). Castillo: Bloqueo de enlaces se debe a ataques a sitios públicos. Retrieved March 19, 2014, from Ultimas Noticias website: http://www.ultimasnoticias.com.ve/noticias/actualidad/politica/castillo-bloqueo-de-enlaces-se-debe-a-ataques-a-pa.aspx

UN. (2014b). Members of the United Nations Security Council. Retrieved April 21, 2014, from United Nations, Security Council website: http://www.un.org/en/sc/members/

United States Court of Appeals. *United States Court of Appeals For the District of Columbia Circuit. Electronic Privacy Information Center Vs. United States Department of Homeland Security*. , (2015).

UNTC. (2016). United Nations Treaty Collection. Retrieved December 16, 2016, from United Nations, Treaty Section website: https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=_en

US Senate. (2011). *Protecting Cyberspace: Assessing the White House Proposal - Senate Hearing 112-221*. Retrieved from http://www.gpo.gov/fdsys/pkg/CHRG-112shrg67638/html/CHRG-112shrg67638.htm

Valeriano, B., & Maness, R. C. (2015). *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Retrieved from https://books.google.com/books?id=HuWkBwAAQBAJ&pg=PA21&lpg=PA21&dq=Cyber+Armageddon+term&source=bl&ots=g94wHnjYwM&sig=_krv9Uj9BQGjXOuN41xvaxErMg0&hl=en&sa=X&ved=0ahUKEwjFoJK6r7XWAhVj1oMKHXGODAgQ6AEIJjAA#v=snippet&q=Armageddon&f=false

Vallier, K., & D'Agostino, F. (2013). Stanford encyclopedia of philosophy. Retrieved April 20, 2017, from Standford Encyclopedia of Philosophy website: https://plato.stanford.edu/entries/justification-public/

Vargas-Leon, P. (2018). National Security Through the Lens of the Internet Kill Switch: An Overview of the Debate in the U.S. and Russia. Retrieved October 13, 2018, from EastWest Institute website: https://www.eastwest.ngo/idea/national-security-through-lens-internet-kill-switch-overview-debate-us-and-russia

Vargas Leon, P. (2015). Tracking Internet Shut Down Practices: Democracies and Hybrid Regimes. In F. Cogburn, Derrick L.; DeNardis, Laura; Levinson, Nanette S.; Musiani (Ed.), *The Turn to Infrastructure in Internet Governance*. Retrieved from http://www.palgrave.com/us/book/9781137533265

Vaughan-Nichols, S. J. (2011, January). How the Internet went out in Egypt. *ZDNet*. Retrieved from http://www.zdnet.com/article/how-the-internet-went-out-in-egypt/

Venables, A. (2019). Establishing Cyber Sovereignty-Russia Follows China's Example. Retrieved March 21, 2019, from RKK ICDS International Centre for Defense and Security website: https://icds.ee/establishing-cyber-sovereignty-russia-follows-chinas-example/

Vendil Pallin, C. (2017). Internet control through ownership: the case of Russia. *Post-Soviet Affairs*, *33*(1), 16–33. https://doi.org/10.1080/1060586X.2015.1121712

Venprensa. (2013). Ministro Arreaza: "Acceso a Internet fue bloqueado por intento de hackeo a la página del CNE" [Minister Arreaza: "Access to Internet was blocked because of an attempt of hacking to the CNE webpage." Retrieved September 28, 2015, from Venprensa website: http://www.venprensa.com.ve/ministro-arreaza-acceso-a-internet-fue-bloqueado-por-intento-de-hackeo-a-la-pagina-del-cne/

Villafranca, L. (2013). Hubo fraude electoral en Venezuela, concluye Instituto de Estudios Europeos. *Noticias Caracol*.

Villarroel, C. (2015). Conatel idea plan para modernizar el Internet [Conatel plan to modernize Internet]. Retrieved March 20, 2017, from El Mundo website: http://www.elmundo.com.ve/noticias/economia/politicas-publicas/conatel-idea-plan-para-modernizar-el-internet.aspx

Vuori, J. A. (2008). Illocutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders. *European Journal of International Relations*, *14*(1), 65–99. https://doi.org/10.1177/1354066107087767

Waddell, K. (2016a). Iraq Shut Down Its Internet to Prevent Sixth-Graders From Cheating. Retrieved from The Atlantic website: http://www.theatlantic.com/technology/archive/2016/05/iraq-shut-down-its-internet-to-prevent-sixth-graders-from-cheating/482946/

Waddell, K. (2016b). The Global Economic Damage of Internet Blackouts. Retrieved October 6, 2016, from The Atlantic website: http://www.theatlantic.com/technology/archive/2016/10/the-global-economic-damage-of-internet-blackouts/503093/

Waever, O. (1995). Securitization and desecuritization. In R. D. Lipschutz (Ed.), *On Security* (Columbia U, pp. 46–86). Retrieved from https://books.google.com/books/about/On_Security.html?id=nI3KmIr5j5MC

Waever, O. (2003). *Securitisation: Taking stock of a research programme in Security Studies*. Retrieved from https://www.clisec.uni-hamburg.de/en/pdf/data/waever-2003-securitisation-taking-stock-of-a-research-programme-in-security-studies.pdf

Walker, R. W. (2010a). Rockefeller calls for public-private action on cybersecurity. Retrieved August 10, 2017, from GCN website: https://gcn.com/articles/2010/04/30/rockefeller-cybersecurity-bill.aspx

Walker, R. W. (2010b). Rockefeller calls for public-private action on cybersecurity. Retrieved August 13, 2017, from FCW website: https://fcw.com/articles/2010/04/30/rockefeller-cybersecurity-bill.aspx

Wang, L. (2003). Protecting BGP Routes to Top-Level DNS Servers. *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, *14*, 851–860.

Ward, M. (2014). Decentralized DNS: Politics of the Domain Name System. Retrieved October 1, 2016, from LIB NETWORK website: https://letstalkbitcoin.com/blog/post/decentralized-dns-politics-of-the-domain-name-system

Waterman, R. (2009). The Administrative Presidency, Unilateral Power, and the Unitary Executive Theory. *Presidential Studies Quaterly*, *39*(1). Retrieved from https://www-jstor-org.libezproxy2.syr.edu/stable/23044871?pq-origsite=summon&seq=1#metadata_info_tab_contents

Watson, P. J. (2013). Russian Cyberspace Head Calls For Internet Kill Switch Alex Jones' Infowars: There's a war on for your mind! Retrieved August 28, 2013, from Infowars website: http://www.infowars.com/russian-cyberspace-head-calls-for-internet-kill-switch/

WB. (2017). Internet Users (per 100 people). Retrieved March 16, 2017, from The World Bank website: http://data.worldbank.org/indicator/IT.NET.USER.P2?locations=CO&view=chart

Weinberger, S. (2013). Cyber Pearl Harbor: Why hasn't a mega attack happened? Retrieved February 17, 2017, from BBC website: http://www.bbc.com/future/story/20130820-cyber-pearl-harbor-a-real-fear

West, D. M. (2016). Internet shutdowns cost countries $2.4 billion last year. Retrieved October 7, 2016, from Brookings Institution website: https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/

White House. (2009). Remarks by the President on Securing Our Nation's Cyber Infrastructure | The White House. Retrieved September 15, 2013, from The White House - Office of the Press Secretary website: http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

Whittaker, Z. (2013). Homeland Security must disclose cell network "kill switch" protocols, court says | ZDNet. Retrieved April 18, 2014, from ZDNet website: http://www.zdnet.com/homeland-security-must-disclose-cell-network-kill-switch-protocols-court-says-7000023217/

Williams, C. (2011). Cameron told not to shut down internet. Retrieved February 3, 2014, from The Telegraph website: http://www.telegraph.co.uk/technology/news/8862335/Cameron-told-not-to-shut-down-internet.html

Williams, M. C. (2003). Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly*, *47*(4), 511–531. https://doi.org/10.1046/j.0020-8833.2003.00277.x

Wilson, N. (2014). Australia's National Broadband Network – A cybersecure critical infrastructure? *Computer Law & Security Review*, *30*(6), 699–709. https://doi.org/10.1016/j.clsr.2014.09.003

Winder, D. (2011). Could the British Government switch off our internet? Retrieved March 20, 2014, from alphr website: http://www.pcpro.co.uk/features/365407/could-the-british-government-switch-off-our-internet

WIPO. (2008). Turkey: Law No. 5651 on Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting. Retrieved December 29, 2014, from WIPO website: http://www.wipo.int/wipolex/en/details.jsp?id=11035

Wood, P. (n.d.). Introduction to the Internet. Retrieved February 2, 2019, from Internet and Web Technologies website: http://www.dcs.bbk.ac.uk/~ptw/teaching/IWT/internet-intro/notes.html

Woolcock, M. (2014). *Engaging with Fragile and Conflict-Affected States.* (No. RWP14-038). Retrieved from file:///C:/Users/Patricia/Downloads/RWP14-038_Woolcock.pdf

WSIS. (2015). *Russian Formal Input: General Assembly's overall review of the implementation of WSIS outcomes Official Form for Comments on the zero-draft Title: Counsellor for Science and Technologies*. Retrieved from http://workspace.unpan.org/sites/Internet/Documents/UNPAN95531.pdf

Xinhua. (2011). Britain's U-turn Over Web-Monitoring. Retrieved November 5, 2018, from CHINADAILY Europe - From Chinese Press website: http://europe.chinadaily.com.cn/opinion/2011-08/15/content_13121232.htm

Yin, R. (2003). *Case study research : design and methods*. Thousand Oaks Calif.: Sage Publications.

Yin, R. (2009). *Case study research : design and methods* (4th ed.). Retrieved from http://www.worldcat.org/title/case-study-research-design-and-methods/oclc/611975393&referer=brief_results

Yin, R. (2014). Case Study Research: Design and Methods. In *SAGE* (5th ed.).

Yoo, T. (2017). The Australian government has created a cybersecurity hub to share intelligence with the private sector. Retrieved March 4, 2017, from Business Insider Australia website: http://www.businessinsider.com.au/the-australian-government-has-created-a-cybersecurity-hub-to-share-intelligence-with-the-private-sector-2017-2

York, K. (2016). Dyn Statement on 10/21/2016 DDoS Attack. Retrieved October 23, 2016, from Dyn Blog website: http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

YouTube. (2014). Venezuela: gobierno no descarta reformas a la Ley RESORTE. Retrieved from https://www.youtube.com/watch?v=91MbwLZcxss

Zavyalova, V. (2014, September 22). Kremlin weighs options for isolating Russian internet in event of crisis. *Russia Beyond the Headlines*. Retrieved from http://rbth.com/science_and_tech/2014/09/22/kremlin_weighs_options_for_isolating_russian_internet_in_eve_39997.html

Zeldin, W. (2014, February 24). Turkey: Law on Internet Publications Amended. Retrieved November 10, 2015, from Global Legal Monitor - Library of Congress website: http://www.loc.gov/law/foreign-news/article/turkey-law-on-internet-publications-amended/

Zmijewski, E. (2014). Turkish Internet Censorship Takes a New Turn. Retrieved March 30, 2016, from Dyn Research | The New Home Of Renesys website: http://research.dyn.com/2014/03/turkish-internet-censorship/

Zuckerman, L. (2015). Por fin se está rompiendo el monopolio de Slim 2015/07/02. Retrieved March 21, 2017, from Excélsior website: http://www.excelsior.com.mx/opinion/leo-zuckermann/2015/07/02/1032474

Curriculum Vitae
Patricia A. Vargas-Leon
Ph.D.

School of Information Studies
221 Hinds Hall
Syracuse University
Syracuse, NY 13244

pavargas@syr.edu
patricia.vargasleon@yale.edu
https://ischool.syr.edu/people/directories/view/pavargas/
Twitter: @patriciaavl
http://syr.academia.edu/PatriciaVargas

EDUCATION

Syracuse University, School of Information Studies. Syracuse, N.Y.
Ph.D. - Information Science and Technology, May 2019
Syracuse University, School of Information Studies. Syracuse, N.Y.
M.Phil. Information Studies, 2014
M.S. Library and Information Sciences, Specialization in Legal Research, School of Information Studies, 2009
Pontifical Catholic University of Peru. Lima, Peru
Lawyer (Expertise: International Law and Law of the Sea), Law School, 2001

FELLOWSHIPS

Information Society Project (ISP) – Yale Law School
Visiting Fellow, New Haven, CT, USA, Yale University, (September 2017 – present)
Cyber SSIG - South School on Internet Governance – 2018 (accepted)
Fellow, Washington D.C., U.S.A., Organization of American States (OAS), April 2018
South School on Internet Governance (SSIG)
Fellow, Rio de Janeiro, Brazil, Getulio Vargas Foundation (FGV), April 2017
Telecommunications Policy Research Conference (TPRC)
TPRC's Graduate Student Consortium, Arlington, Virginia, U.S.A. 2016
Google
Policy Fellow, Buenos Aires, Argentina, Summer 2014
European Summer School on Internet Governance (Euro-SSIG)
Fellow, Maissen, Germany, Summer 2013

TEACHING AND RESEARCH EXPERIENCE

Syracuse University, School of Information Studies

Teaching Activities (2010-2015)

- Adjunct Instructor - Information Policy (IST 618), (2015)
- Teaching Assistant - Doctoral Gateway course Doctor of Professional Studies in Information Management Program (IST 801), (2011)
- Teaching Assistant - Information and Information Environments (IST 601) (2011)
- Teaching Assistant - Information Policy (IST 618), (2010)

Research Assistant (2011-2015)

- Worked in "big data" project: analysis of the impact of social networks on political campaign

- Worked on data collection for projects of cyber-security, social network analysis, conflict of jurisdictions in the cyberspace, Internet fragmentation and Internet critical resources
- Collected and analyzed data performing qualitative analysis using Atlas-Ti and N-Vivo
- Wrote literature reviews and research papers

PUBLICATIONS

Book Chapters

Vargas Leon, P. (2016). Net Neutrality: An Overview of Enacted Laws in South America. In P. Bell, Luca; De Filippi (Ed.), Net Neutrality Compendium. SPRINGER.

Vargas Leon, P. (2015). Tracking Internet Shut Down Practices: Democracies and Hybrid Regimes. In F. Cogburn, Derrick L.; DeNardis, Laura; Levinson, Nanette S.; Musiani (Ed.), The Turn to Infrastructure in Internet Governance. Palgrave Macmillan.

Journal Articles

Vargas-Leon, P. A., & Kuehn, A. (2015). The Battle for the Critical Internet Resources: South America vs. Amazon. The Law, State and Telecommunications Review / Revista de Direito, Estado E Telecomunicações, 7(1), 37–58.

Garcia-Murillo, M., Velez-Ospina, J. A., & Vargas-Leon, P. (2013). The Techno-Institutional Leap and the Formation of New Firms. Journal of Information Policy, 3, 501. http://doi.org/10.5325/jinfopoli.3.2013.0501

Vargas-Leon, Patricia (2005). El límite marítimo entre Perú y Chile: un problema aún sin solución [Sea boundaries between Peru and Chile: a problem without solution]. Revista de Derecho Foro Jurídico, 2(4), 229-234.

PROCEEDINGS

Vargas-Leon, Patricia & Badiei, Farzaneh (2017). A Practical Guide to Applying the Law of the Sea into the Internet: Where the Internet Root Zone and the High Seas Find Each Other.
Internet Law Works-in-Progress, Spring 2018 – New York Law School, New York (accepted)

Vargas-Leon, Patricia & Badiei, Farzaneh (2017). A Practical Guide to Applying the Law of the Sea into the Internet: Where the Internet Root Zone and the High Seas Find Each Other.
TPRC (Research Conference on Communications, Information and Internet Policy), Fall 2017 – Virginia, U.S.A.

Vargas-Leon, Patricia (2017). Implications of the application of the UNCLOS delimitation policy, a case study for the "hot pursuit" principle in the cyberspace.
International Studies Association (ISA), Spring 2017 - Maryland, U.S.A.

Vargas-Leon, Patricia (2016). Implications of the application of the "hot pursuit" principle in the cyberspace: an analysis of the case "Microsoft v. United States of America"
Global Internet Governance Academic Network (GigaNet). A Global Network for Scholars of Internet Governance, Fall 2016 – Guadalajara, Mexico

Vargas-Leon, Patricia (2016). Implications of the Application of the 'Hot Pursuit' Principle in the Cyberspace: An Analysis of the Case “Microsoft v. United States of America”
TPRC (Research Conference on Communications, Information and Internet Policy), Fall 2016 – Virginia, U.S.A.

Vargas-Leon, Patricia (2016). Tracking Internet Shut Down Practices: Democracies and Hybrid Regimes
ISA (International Studies Association Conference), Spring 2016 – Georgia, U.S.A.

Vargas-Leon, Patricia (2015). Securitization of the Critical Infrastructure: a case study for the "Internet shutdown"
ISA (International Studies Association Conference), Spring 2015 – New Orleans, U.S.A.

Vargas-Leon, Patricia (2014). Net Neutrality: An Overview of Enacted Laws in Latin America. Net Neutrality: An Ongoing Regulatory Debate. 2nd Report of the Dynamic Coalition on Network Neutrality.
IGF (Global Internet Governance Network/Internet Governance Forum) Fall 2014 – Istanbul, Turkey

Vargas-Leon, P. A., & Kuehn, A. (2014). The Battle for the Critical Internet Resources: South America vs. Amazon. Political Economy of Critical Internet Resources: South America vs. Amazon, Inc.: The battle for .AMAZON
GIGANET/IGF (Global Internet Governance Network/Internet Governance Forum) Fall 2014 – Istanbul, Turkey

Vargas-Leon, Patricia (2013). The evolution of the legislative proposals about the "Internet Kill Switch" in the U.S.A: a historic-legal analysis
GIGANET/IGF (Global Internet Governance Network/Internet Governance Forum) Fall 2013 – Bali, Indonesia

Vargas-Leon, Patricia (2012). Monitoring social networks in the first nation-state that achieved a network neutrality law, a case-study in Chile
Award for the project: PLACA-Moynihan Institute Summer Grant (Syracuse University)
ACORN-REDECOM (Americas Communication Research Network- Red Americana de Investigación e Información y Comunicación) Summer 2013 – Mexico City, Mexico

Garcia-Murillo, M., Velez-Ospina, Javier & Vargas –Leon, P.A. (2012). Where should governments invest? The impact of economic, political, social and technological factors on the formation of new firms
Syracuse University, School of Information Studies
Dr. Martha Garcia-Murillo, Principal Investigator
ACORN-REDECOM (Americas Communication Research Network- Red Americana de Investigación e Información y Comunicación) Summer 2012 – Valparaiso, Chile

PANEL

Kuehn, A. Vargas–Leon, P.A. & DeNardis, L. (2014). Politics, Publics, Participation and Practices: Governance of Technologies in Global Networks
4S / ESOCITE (Society for Social Studies of Science) Summer 2014 - Buenos Aires, Argentina

INVITED PRESENTATIONS

Analyzing Governments' Regulatory Practices Over Global Resources: Comparing the Law of the Sea and the Cyberspace. Presentation delivered in the Workshop on Political Space and Cyberspace, Georgia Institute of Technology School of Public Policy, Georgia Tech, May 19-20, 2016.
Co-sponsors: Internet Governance Project (IGP), Texas A&M

Addressing the Ultimate Form of Cybersecurity Control: A Multiple Case Study for the "Internet Kill Switch". Presentation delivered to the Annenberg School for Communication, University of Pennsylvania, March 18th, 2015.

SERVICE DISCIPLINARY

Book Manuscript Reviewing
Book Manuscript Reviewing, Fall 2016
MIT Press, Massachusetts Institute of Technology (MIT)
Conference Service
IGF – Internet Governance Forum, December 2018
Session Trade Agreements and the Internet, on-Site Moderator

IGF – Internet Governance Forum, December 2016
Main Session Trade Agreements and the Internet, on-Site Moderator
TPRC - Telecommunications Policy Research Conference, Fall 2012-2013
Professional Service
ACORN-REDECOM (Americas Communication Research Network- Red Americana de Investigación e Información y Comunicación), now known as CPR-LATAM, Fall 2010 – Spring 2013
Professional Service,
Syracuse University
Professional Service, Fall 2010- Spring 2012

PROFESSIONAL WORK EXPERIENCE

Program Assistant, School of Information Studies, Syracuse University (2010-2012)

- Worked in academic and administrative functions for the distance academic program of the School of Information Studies
- Evaluated candidates to be admitted into the Doctor of Professional Studies
- Participated as member of the Doctoral Committee at the School of Information Studies

Information Consultant – United Nations Division of Ocean Affairs and Law of the Sea (DOALOS) (2009-2010)

- Worked on research legal consultation: sovereignty, jurisdiction, maritime controversy and agreements between nation-states
- Implemented an electronic system for the reference collection and cataloging system of the division

Research Assistant of the Telecommunications and Network Management Program, School of Information Studies, Syracuse University - (2008 -2011)

- Analyzed telecommunication policies and the role of regulators in the Americas
- Analyzed policies related to innovation and regulation in the Telecommunications Sector

Legal Consultant in Corporate Law – Private Corporation "Desarrollo Total S.A.C." [Total development S.A.C.]. Lima, Peru (2004-2005)

- Worked on corporate private transactions

Civil servant - Oficina Nacional de Registros Públicos de Lima, Peru [National Office of Public Records from Lima, Peru] (2003)

- Evaluated and classified legal aspects of private transactions

- Wrote final resolutions and reports for public users

Independent Legal Consultant (2001-2006)

- Worked in civil, telecommunications and corporate cases
- Worked in research projects related to international law jurisprudence

Legal assitant - Law Firm “Solución Legal para Empresas” - SOLEGSA [Legal Solution for Corporations], Lima, Peru (1999-2000)

- Worked as a legal assistant in areas of Telecommunications, Civil, Administrative, Commercial and Corporate Law

ACADEMIC HONORS

- Inducted into National Scholar Honor Society – Magna Cum Laude (May 2009)
- Merit-based Graduate Assistantship. School of Information Studies, Syracuse University (2008-2009 / 2010-2015)
- Pontifical Catholic University of Peru "Fifth Superior," for the Top 10% of the best students (July 1998)

LANGUAGES

Spanish: Mother tongue
English: Advanced level
French: Intermediary level

LEADERSHIP ACTIVITIES

BOOST INITIATIVE - Bolstering Original Opportunity and Self Through Technology
Syracuse University, NY
Recognitions for the project:
Grant Kauffman Foundation
Syracuse University Chancellor’s Award - April 2009