Addressing the ultimate form of cyber security control: a multiple case study for the Internet kill switch

Patricia Vargas-Leon[1]
[1]Syracuse University

Abstract
The purpose of this project is to study a policy called "shutdown of the Internet." Preliminary findings show that this policy is a form of governmental control that has been used or considered by both, democratic and non-democratic governments, in the name of national security. This project adopts the securitization theory of the Copenhagen School and uses a multiple case study approach to analyze the arguments democratic and hybrid regimes use to justify shutting down the Internet. Data collection followed an Internet search process analyzing news, political speech and national statutes related to telecommunications law. Collected documents were coded and analyzed according the categories of the rhetorical speech using computer-assisted qualitative data analysis software. The research questions are: RQ1: What is the global scope of the Internet shut down phenomena? RQ2: What justifications do democratic and hybrid regimes use to shut down or to consider shutting down the Internet?
Keywords: Internet, Internet kill switch, Internet shutdown, Copenhagen securitization theory
doi: 10.9776/16565

Contact: pavargas@syr.edu

1. Introduction

Governments worldwide have tried to control the Internet infrastructure and have adjusted their national statutes to enable these actions. Between 1995 and 2011, there were over 600 instances of government control over digital networks made by consolidated and unconsolidated democracies, authoritarian regimes and fragile states (Howard, Agarwal, & Hussain, 2011). One of these actions of governmental control was an Internet shutdown, the most extreme form of control over the Internet infrastructure. Earliest findings of this policy go back to 2005, and empirical evidence shows three possible ways it is used or might be used:

a) by governments to deprive their own population from having Internet access, b) by governments to deprive different populations (other than their own) from having Internet access (as tool of cyber-warfare) and c) by private citizens or organizations to deprive specific populations from Internet access. This project will focus on attempts by governments to deprive their own populations from having Internet access for reasons of national security.

2. Internet shutdown: a.k.a. "internet kill switch"

Shutting down the Internet is defined as a government attempt to stop all Internet activity, and is colloquially known as the "Internet kill switch" (Opderbeck, 2012).
The literature defines both terms from three perspectives:

a) From a political point of view, as the President's authority to disconnect commercial and private wireless networks when a nation-state faces a national security threat (Liebelson, 2013)
b) From a technical point of view, as the attempt to interrupt all Internet and cellular communication activity (Johnson, 2011)

c) From a cyber-security point of view, as a control mechanism to protect the critical infrastructure when a nation-state faces a cyber-attack (Murray, Zeadally, & Flowers, 2012)

Despite its name, a kill switch device for the Internet does not actually exist. To stop all Internet activity, action must be taken on each of the following elements of the TCP/IP protocol: Internet service providers (ISPs), Internet Exchange Points (IXPs), fiber-optic cables, the Domain Name System (DNS) and the Border Gateway Protocol (BGP) (Chang, 2013; Eagleman, 2012).

3. National Security

National security traditionally 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 determining what issues must be securitized; those issues and are known as “security priorities” (Richards, 2012). Seen as the “national interest,” security priorities may change according to the nation-state’s geopolitical position or external conflicts (Bobbitt, 2002; Richards, 2012).

4. Theoretical Framework

The theoretical framework used in this project is the “Securitization Theory of the Copenhagen School,” also known as “securitization theory”. This theory argues that security is a constructed concept, a specific type of politics applicable to a very broad set of issues in certain time (Buzan, 1998).

The securitization theory defines security as a “speech act that securitizes,” and constitutes one or more “referent objects,” which can be identified as the national interest. This theory has been selected for this project because the political speech about securitization has been oriented to construct “cyber issues” as “security problems,” rather than regular political, economic, illegal or technical problems (Hansen, 2009; Williams, 2003).

Using the terms of the securitization theory, this study has the purpose of exploring the different justifications governments used in shutting down the Internet, an "extreme measure" to protect what they consider the "referent object," in order to guarantee the national security of a nation-state.

The securitization theoretical framework identifies the following elements: a) Securitizing Actor: whoever “securitizes” something, b) Referent Object: thing to be protected, c) Audience: person to be convinced with the security speech and d) Extraordinary Measure: action (s) to protect the referent object.

5. Research Approach

This project is driven by two factors:

a) To challenge the common belief that extreme forms of governmental control are only considered or applied by authoritarian regimes.
b) The need to understand why democracies, self-proclaimed defenders of Internet freedom, used or considered using mechanisms of governmental control that these governments criticized in their official policy discourse.

6. Multiple Case-Study

By using the theoretical constructs of the Copenhagen School, this project will take the form of a multiple case study of five governments that justified shutting down the Internet, or considered doing it, and which provided public justification or legal documents that can be analyzed.

Local legislation, political speech concerning government security and the governmental actions of these five governments will be compared and examined.

This proposed study has two stages:

a) Identification of the Internet shut down episodes worldwide and,
b) Identification of the justifications governments used to shut down the Internet or to consider doing it by analyzing political speech

The following case studies have been selected:

Type of Regime	Well Established Democracy	Hybrid Regimes	Shut Down (s), Considered (c)
Australia	X		S
United Kingdom	X		C
United States	X		C
The Russian Federation		X	C
Venezuela		X	S

Table 1. Proposed Case Studies

Governments were classified as democratic or hybrid regimes following the classification of the Economist Intelligence Unit (EIU) (EIU, 2014). The EIU classification, differently from the classic approach, evaluates a nation-state "democratic status" by considering different categories besides the existence of a national election process: pluralism, civil liberties, functioning of government, political participation and political culture.

7. Research Questions and Data Collection

The specific research questions that drive this project 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?

Data collection followed a deep Internet research process which analyzed:

a) News, articles, websites, blogs, and related artifacts (like videos, podcasts and social media platforms) related to the participation of private telecomm operators or government actions over private Internet infrastructure.
b) Political speech of the securitizing agents
c) National statutes: Internet law, Telecommunications law, Cyber security law, National security law

The collected documents were analyzed and coded following the categories of the rhetorical speech (Purpose, Audience, Persona, Tone, Evidence, Structure, Strategies) by using computer-assisted qualitative data analysis software ATLAS-ti. The purpose of the coding process was to identify the main elements of the theoretical framework as explained in the next paragraph and to provide an answer for RQ2.

8. Preliminary Findings and Conclusion

A preliminary study revealed that, between 2005 and 2015, eleven governments attempted to shut down the Internet: a) nine authoritarian regimes, b) a hybrid regime and c) one well-consolidated democracy. In the same period, two well-consolidated democracies and one hybrid regime considered giving legal protection to this form of government control (Cowie, 2014; Mora, 2014; OpenNet, 2013).

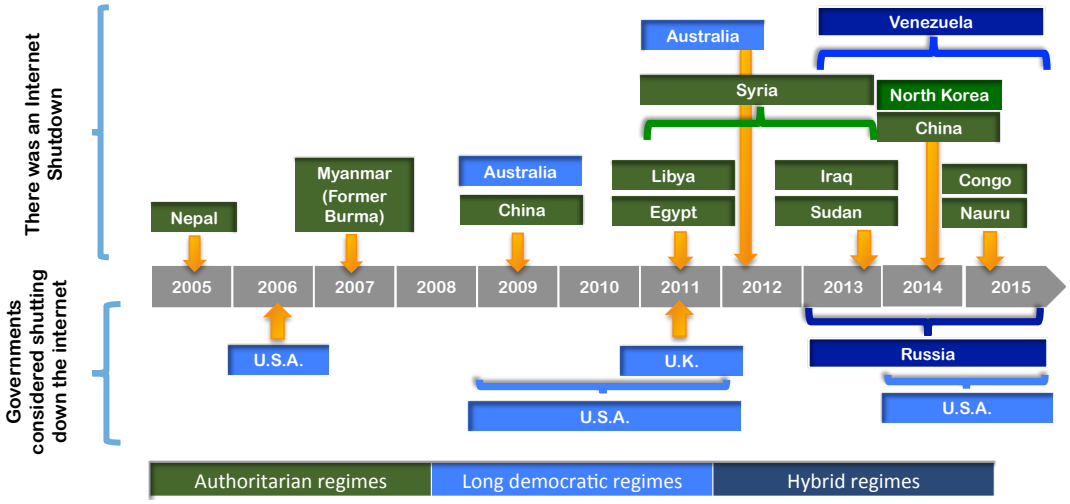

Figure 1. Internet Shut Down Cases

Both, democratic and hybrid regimes justified their actions to control the Internet infrastructure, or their intentions to do so, by citing unclear legislations concerning telecommunications and national security. Members from the Executive and Legislative branches assumed the role of securitizing agents by warning about the Internet as the main threat to the stability of the nation-state, but the decision to shut down the Internet corresponds to a single authority, usually the President. The concept of national interest (or referent object) however, has different meanings for different regimes. Concepts of national interest include: a) the critical infrastructure, b) social control (in time of political unrest) and c) the communication means of the ruling party.

The research analysis suggests that the audiences governments attempt to address belong to the private sector, specifically, the private sector that owns the critical infrastructure and the private sector that controls massive communication means. Governments provided different justifications:

Democratic regimes that considered shutting down the Internet emphasized the protection of the critical infrastructure in case of a cyber-attack, however they also consider this extreme policy as a mechanism of social control when the public order is threatened. Democratic regimes that did use this form of government control claimed that it was an accident and denied their intention to use it for political purposes. Their population challenged that explanation.

Hybrid regimes blame foreign powers for the instability of their regimes and claim an “unclear” national interest threatened by the Internet. These regimes focus on maintaining control over the national information infrastructure and the protection of the communication platforms of the ruling party as their referent object.

From a policy point of view, these preliminary findings show two characteristics: a) depending upon the specific government, the power to order shutting down the Internet is generally concentrated in one governmental authority (usually the Executive branch), but accountability may vary, and b) there are legal frameworks that “legitimize” explicit or implicitly this extreme form of governmental control over the Internet.

Future research will include the study of the Internet shutdown as a form of cyber-warfare and possible implications of this policy on the multi-stakeholder model and the open architecture design of the Internet.

9. References

Bobbitt, P. (2002). *The Shield of Achilles: War, Peace, and the Course of History*. Knopf.
Buzan, B. (1998). *Security : a new framework for analysis*. Boulder Colo.: Lynne Rienner Pub.
Chang, A. (2013). Why Undersea Internet Cables Are More Vulnerable Than You Think | WIRED. Retrieved April 20, 2015, from http://www.wired.com/2013/04/how-vulnerable-are-undersea-internet-cables/
Cowie, J. (2014). Internet kill switch - Renesys. Retrieved March 11, 2014, from http://www.renesys.com/?s=Internet+kill+switch&x=0&y=0
Eagleman, D. (2012). Four ways the Internet could go down - CNN.com. Retrieved March 20, 2014, from http://www.cnn.com/2012/07/10/tech/web/internet-down-eagleman/
EIU. (2014). Special Reports and Multimedia. Retrieved December 6, 2015, from http://www.eiu.com/landing/special_reports
Hansen, L. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155 – 1175.
Howard, P., Agarwal, S., & Hussain, M. (2011). The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks? *Issues in Technology Innovation*, (13). Retrieved from http://www.brookings.edu/~/media/research/files/papers/2011/10/dictators digital network/10_dictators_digital_network.pdf
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
Liebelson, D. (2013). The Government's Secret Plan to Shut Off Cellphones and the Internet, Explained | Mother Jones. Retrieved March 5, 2014, from http://www.motherjones.com/politics/2013/11/internet-phone-kill-switch-explained
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 http://angelicamorabeals.blogspot.com/2014/03/en-venezuela-estado-tachira-sin-internet.html
Murray, A., Zeadally, S., & Flowers, A. (2012). An assessment of US legislation on cybersecurity. *Cyber Security, Cyber …*, 289–294. doi:10.1109/CyberSec.2012.6246106
Opderbeck, D. W. (2012). Does the Communications Act of 1934 Contain a Hidden Internet Kill Switch? *SSRN Electronic Journal*. Retrieved from http://papers.ssrn.com/abstract=2131287
OpenNet. (2013). OpenNet Initiative. Retrieved from https://opennet.net/
Paleri. (2008). *National Security: Imperatives and Challenges*. Tata McGraw-Hill Education. Retrieved from http://books.google.com/books?id=DMzcGe0-HQwC&pgis=1
Richards, J. (2012). *A guide to national security : threats, responses and strategies*. Oxford ;;New York: Oxford University Press.
Williams, M. C. (2003). Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly*, *47*(4), 511–531. doi:10.1046/j.0020-8833.2003.00277.x