Not By Technical Means Alone: The Multidisciplinary Challenge of Studying Information Controls

Masashi Crete-Nishihata*, Ronald J. Deibert, and Adam Senft,
Citizen Lab, Munk School of Global Affairs, University of Toronto

The study of information controls is a multidisciplinary challenge. Technical measurements are essential to such a study, but they do not provide insight into why regimes enact controls or what those controls' social and political effects might be. Investigating these questions requires that researchers pay attention to ideas, values, and power relations. Interpreting technical data using contextual knowledge and social science methods can lead to greater insights into information controls than either technical or social science approaches alone. The OpenNet Initiative has been developing a mixed-methods approach to the study of information controls since 2003. This article presents our approach through a series of case studies and concludes with a discussion of methodological challenges and recommendations for the field moving forward.

*corresponding author
315 Bloor Street West.
Toronto, ON, M5S 1A3Canada
masashi (at) citizenlab.org
https://citizenlab.org

This article appears in IEEE Internet Computing, vol. 17, no. 3, pp. 34-41, May-June 2013,

Suggested Citation: Masashi Crete-Nishihata, Ronald Deibert, Adam Senft, "Not by Technical Means Alone: The Multidisciplinary Challenge of Studying Information Controls," IEEE Internet Computing, vol. 17, no. 3, pp. 34-41, May-June 2013, http://doi.ieeecomputersociety.org/10.1109/MIC.2013.29

Information controls can be conceptualized as actions conducted in and through the Internet and other information and communication technologies (ICTs). Such controls seek to deny (as with Internet filtering), disrupt (as in distributed-denial-of-service (DDoS), attacks), or monitor (such as passive or targeted surveillance) information for political ends. Here, we examine national-level, state-mandated Internet filtering, but the arguments we raise apply to other information controls and technologies as well.

Technical measurements are essential for determining the prevalence and operation of information controls such as Internet filtering. However, alone, such measurements are insufficient for determining why regimes decide to enact controls and the political, social, and economic impacts of these decisions. To gain a holistic understanding of information controls, we must study technical processes and the underlying political, legal, and economic systems behind them. Multiple actors in these systems seek to assert agendas and exercise power, including states (military, law enforcement, and intelligence agencies), civil society, and the private sector. These actors have different positions of influence within technical, political, and legal systems that affect their motivations and actions, as well as the resulting consequences. At its core, the study of information controls is a study of ideas, values, and interests that motivate actors and the power relations among those actors. The Internet is intimately and inseparably connected to social relations and thus grounded contexts, from its physical configuration -- which is specific to each country -- to its political, social, and military uses. Studying the technical operation of information controls and the political and social context behind them is an inherently multidisciplinary exercise.

In 2003 the OpenNet Initiative (ONI; https://opennet.net), an interuniversity consortium, was launched with the mission of empirically documenting national-level Internet censorship through a mixed-methods approach that combines technical measurements with fieldwork, legal, and policy analysis. At the time, only a few countries filtered the Internet. Since 2003, the ONI has tested for Internet filtering in 74 countries and found that 42 of them -- including both authoritarian and democratic regimes -- implement some level of filtering.[1] Internet censorship is quickly becoming a pervasive global norm. The spread and dynamic character of information controls makes the need for evidence-based multidisciplinary research on these practices increasingly important. Here, we present the ONI approach through several case studies and discuss methodological challenges and recommendations for the field moving forward.

Mixed Methods Approach

Despite the global increase in Internet censorship, multidisciplinary studies have been limited. Technical studies have focused on specific countries (such as China) and filtering technologies.[2] Studies of global Internet filtering have used PlanetLab (https://planet-lab.org), which has limited vantage points into countries of interest and tests on academic networks which might not represent average national level connectivity.[3] In the social sciences, particularly Political Science and International Relations, empirical studies on information controls and the impact of the Internet on global affairs are growing, but seldom use technical methods. This slow adoption is unsurprising; disciplinary boundaries are deeply entrenched, and incentives to explore unconventional methods, especially ones that require specialized skills, are low. Social scientists are more comfortable focusing on social variables: norms, rules, institutions, and behaviours. While these variables are universally relevant to social science, for information controls research they should be paired with technical methods, such as network measurements.

Studying information controls requires skills and perspectives from a range of disciplines including computer science (especially network measurement and security), law, political science, sociology, anthropology, and regional studies. Gaining proficiency in all of these fields is difficult for any scholar or research group. We attempted to bridge these areas through a multidisciplinary collaboration. The ONI started as a partnership between the University of Toronto, Harvard University, and the University of Cambridge, bringing together researchers from political science, law, and computer science. Beyond these core institutions, the ONI helped form and continues to support two regional networks, OpenNet Asia (http://opennet-asia.net) and OpenNet Eurasia.[4] Fieldwork conducted by local and regional experts from our research network has been a central component of our approach. The practice and policy of information controls can vary widely between countries. Contextual knowledge from researchers who live in the countries of interest, speak the local language, and understand the cultural and political subtleties, is indispensable.

Our methods and tools for measuring Internet filtering have evolved gradually over the past ten years. Early efforts used publicly available proxies and dial-up access to document filtering in China.[5] A later approach (which continues today) is client-based in-country testing. This approach uses software written in Python in a client-server model, which is distributed to researchers. The client attempts to access a pre-defined list of URLs simultaneously in the country of interest (the “field”) and in a control network (the “lab”). In our tests, the lab connection was the University of Toronto network, which does not filter the type of content we test for. Once the tests have completed, the results are compressed and transferred to a server for analysis. A number of data points are collected for each URL access attempt: HTTP headers and status code, IP address, page body, and in some cases traceroutes and packet captures. A combined process of automated and manual analysis attempts to identify differences in the results returned between the field and lab and isolate instances of filtering. As attempts to access websites from different geographic locations can return different data points for innocuous reasons (such as a domain resolving to different IP addresses for load balancing, or displaying content in different languages depending on where a request originates from) manual inspection of results is often necessary.

Internet censorship research involves ethical considerations, particularly when client-based testing is employed.[6] Client-based testing involves openly accessing a large number of potentially sensitive websites in quick succession, which may pose security concerns for users depending on the location. As our goal is to reproduce and document the experience of an average Internet user in the country of interest, the client does not use censorship circumvention or anonymity techniques when conducting tests. Before testing takes place, we hold an informed consent meeting to clearly explain the risks of participating in the research. The decision of where to test is driven by concerns for safety and practicality. Often countries with the potential for interesting data are considered too dangerous for client-based testing. For example, due to security concerns we have not run client-tests during Syria's recent conflict, or in certain countries altogether (e.g. Cuba and North Korea).

Internet filtering measurements are only as good as the data sample being tested. ONI testing typically uses two lists of URLs as our sample: a global list and a local list. The global list comprises a range of internationally relevant and popular websites, predominantly in English, such as international news sites (e.g. CNN, BBC, etc) and social networking platforms (e.g. Facebook and Twitter). It also includes content that is regularly filtered, such as pornography and gambling sites. This list acts as a baseline sample that allows for cross-country and cross-temporal comparison. Local lists are compiled for each country by regional experts, and have material specific to the local political, cultural, and linguistic context. These lists can include URLs of local independent media, oppositional political and social movements, or religious organizations unique to a country or region of interest. The lists also contain URLs that have been reported to be blocked or have content likely to be targeted in that country. These lists do not attempt to enumerate every website that a country might be filtering, but they can provide a snapshot into filtered content's breadth, depth, and focus.

Before testing occurs, gaining knowledge about the testing environment, including a country's Internet market and infrastructure, can help determine significant network vantage points. Understanding a country's regulatory environment can provide insight into how it implements information controls, legally and extra-legally, and how ISPs might differ in implementing filtering.

Timing in testing is also important. Authorities might enact or alter information controls in response to events on the ground. Because our testing method employs client-based testing and analysis, resource constraints require that we schedule testing strategically. Local experts can identify periods in which information might be disrupted, such as elections or sensitive anniversaries, and provide context for why events might trigger controls.

Case Studies

The intentions and motivations of authorities who mandate censorship are not readily apparent from technical measurements alone. Filtering might be motivated by time-sensitive political events, and can be implemented in a non-transparent manner for political reasons. In other cases, decisions to filter content might come from a desire to protect domestic economic interests. Filtering can also come with unintended consequences when the type of content filtered and the jurisdiction where it is blocked are not the censors' intended targets.

In the following cases, we illustrate how a mixed-methods approach can ground technical filtering measurements in the political, economic, and social context in which authorities apply them.

Political Motivations

Although technical measurements can determine what is censored and how that censorship is implemented, they cannot easily answer the question of why content is censored. Understanding what motivates censorship can provide valuable insight into measurements while informing research methods.

Political Events

Information controls are highly dynamic and can be triggered or adjusted in response to events on the ground. We call this practice just-in-time blocking (JITB), which refers to the denial of access to information during key moments when the information might have the greatest impact, such as during elections, periods of civil unrest, and sensitive political anniversaries.[7]

The most dramatic implementation of JITB is the complete shutdown of national connectivity as seen recently during mass demonstrations in the Middle East and North Africa (MENA).[8] In these extreme cases, the disruption can be seen via traffic monitoring, while the political event's prominence makes the context obvious. In other cases the disruption may be subtle and only implemented for a short period. For example, ONI research during the 2005 Kyrgyzstan parliamentary elections and 2006 Belarus presidential elections found evidence of DDoS attacks against opposition media and intermittent website inaccessibility.[9] In these cases attribution is difficult to assess; attacks such as DDoS provide a level of plausible deniability.

Recurring events (e.g. sensitive anniversaries) or scheduled events (e.g. elections) provide opportunities to trace patterns of information controls enacted in response to those events. As our client-based testing relies on users in country, continuous monitoring is not feasible, and knowledge of events that may trigger information controls is highly valuable. However, even in countries with aggressive information controls and records of increasing controls during sensitive events, anticipating which events will lead to JITB can be difficult.

In 2011, we collaborated with the British Broadcasting Corporation (BBC) to analyze a pilot project the BBC conducted to provide web-proxy services to deliver content in China and Iran, where BBC services have been consistently blocked.[10] We monitored the usage of Psiphon (the proxy service used by the BBC; see https://psiphon.ca) and tested for Internet filtering daily before, during, and after two anniversaries of sensitive political events: the 1989 Tiananmen Square protest and 2009 disputed Iranian presidential elections. Due to the sensitivity of the anniversaries and past evidence of the regimes targeting information controls around the anniversary dates, we hypothesized that authorities would increase controls around the events. However, our hypothesis was not confirmed -- we observed little variance in blocking and no secondary reports of increased blocking. We also did not observe the expected increase in blocking of Psiphon nodes. However, a number of unforeseen events in China did appear to trigger a censorship increase. Rumours surrounding the death of former President of the People's Republic of China, Jiang Zemin and public discontent following a fatal train collision in Wenzhou were correlated with an increase in the blocking of BBC's proxies and other reports of censorship. Other studies have similarly shown Chinese authorities quickly responding to controversial news stories with increased censorship of related content.[11] This case shows that predicting changes in information controls is difficult and unforeseen events can rapidly influence how authorities target content. Measurement methods that are technically agile, can adapt to events, and are informed by a rich understanding of the local context through local experts can help reduce this uncertainty.

Filtering Transparency

The degree to which censors acknowledge that filtering is taking place and inform users what content is filtered can vary significantly between countries and ISPs. Many states apply Internet filtering openly with explicit block pages that notify users why content is blocked and in some cases offer channels to appeal a block. Others apply filtering using methods that make websites appear inaccessible due to network errors, with no acknowledgement that access has been restricted and no remedies offered to users. Interestingly, in some cases filtering is applied transparently to certain types of content and covertly to others.

Although determining filtering transparency is a relatively straightforward technical question, knowing what motivates censors to make filtering more or less transparent requires knowledge of the environment in which such filtering takes place. States may filter transparently in an effort to be perceived as upholding certain social values, as seen among MENA countries that block access to pornography or material deemed blasphemous. Other states may wish to retain plausible deniability to accusations that they block sites of opposition political groups, and thus might block using methods that mimic technical errors to the user.

Yemen's filtering practices illustrate this complexity. ONI testing in Yemen found that some content, including pornography and LGBT material, are blocked with an explicit block page outlining why the content was blocked and offering an option to have this blocking re-assessed.[12] However, other websites, particularly those containing critical political content, have been consistently blocked through TCP reset packet injection. This method is not transparent to an average user and would be difficult to distinguish from routine network issues. State-run ISPs in Yemen have denied these political sites are blocked, instead attributing their inaccessibility to technical error.

We thus see variability in the transparency of filtering, with some websites blocked openly and others filtered covertly, which leaves an average user uncertain as to the cause of a website's inaccessibility. While the methods of blocking are readily apparent from the technical data gathered, what is not as clear from data alone are the political and social dynamics which lead to the use of different blocking methods. Covertly blocking political content offers the government plausible deniability that it is censoring political opposition and critical speech, which is ostensibly protected by Yemen's constitution. Other content, such as pornography, is blocked openly based on Sharia law, which forms the source of legislation in Yemen's constitution.

Other countries similarly vary in how openly content is filtered and how closely filtering aligns with the country's stated motivations for censorship. Vietnam, for example, has historically claimed that information controls were intended to limit access to pornography.[13] However, Vietnam extensively blocks critical political and human rights content through DNS tampering. Similarly, the Ethiopian government has previously denied blocking sensitive content, despite our findings of blocking of political blogs and opposition parties' websites.[14] These examples show that national-level filtering systems justified by authorities to block specific content like pornography may be extended through "mission creep" to include other sensitive material in unaccountable and non-transparent ways.[15]

Economic Motivations

Economic factors also help determine what authorities censor and how they apply that censorship. In countries with strict censorship regimes, the ability to offer unfettered access can provide significant competitive advantage or encourage investment in a region. Conversely, targeting particular services for filtering while letting others operate unfettered can protect domestic economic interests from competition. Economic considerations might also affect the choice of filtering methods.

ONI research in Uzbekistan has documented significant variation in Internet filtering across ISPs.[16] Although many ISPs tested consistently filtered a wide range of content, others provided unfiltered access. The technical data alone could not explain this result. Contextual field-work determined that some commercial ISPs had close ties with the president's inner circle, which might have helped them resist pressure to implement filtering. This relationship let the ISPs engage in economic rent-seeking, in which they used their political connections to gain a competitive advantage by offering unfettered access.

Other instances show how economic interests shape the application of information controls. Until 2008, the United Arab Emirates' (UAE) ISP Du did not filter, while Etisalat, the country's other major ISP, filtered extensively.[17] Like the case of Uzbekistan, this variation was motivated by economic interests. Du serves the majority of customers in UAE's economic free zones, set up to encourage the development of technology and media sectors. The provision of unfettered access was an incentive to attract investment.

Conversely, some online services might be filtered to protect commercial interests. Countries including the UAE and Ethiopia filter access to, and have passed regulations restricting the use of, VoIP services such as Skype to protect the interests of national telecommunications companies, a major source of revenue for the state.

The decision to implement a particular filtering method may also be influenced by cost considerations as much as technical concerns. Some filtering methods, such as IP blocking, can be implemented on standard network equipment. Other more technically complex methods, such as TCP reset packet injection, require more sophisticated systems.

Unintended Consequences

In some instances, states might apply filtering in a way that blocks content not intentionally targeted for filtering, or affects jurisdictions outside of where the filtering is implemented. Such cases can be difficult to identify from technical measurement alone.

Upstream filtering

The Internet's borderless nature complicates research into national-level information controls. Internet filtering, particularly where it is not implemented transparently, can have cross-jurisdictional effects that are not immediately apparent.

We can see this complexity in upstream filtering in which filtering that originates in one jurisdiction ends up applied to users in a separate jurisdiction. If ISPs connect to the broader Internet through peers that filter traffic, this filtering could be passed on to users. In some cases, an underdeveloped telecommunications system might limit a country's wider Internet access to just a few foreign providers, who might pass on their filtering practices. Russia, for example, has long been an important peer to neighboring former Soviet states and has extended filtering practices beyond its borders. The ONI has documented upstream filtering in Kyrgyzstan, Uzbekistan, and Georgia.[18]

In a recent example, we found filtering applied by ISPs in India was restricting content to users of the Omani ISP Omantel.[19] Through publicly available proxies and in-country client-based testing we collected data on blocked URLs in Oman, a country with a long history of Internet filtering. While our results showed that users attempting to access blocked content were presented with a number of different block pages, one of the block pages presented to users was not consistent with past filtering employed by ISPs in Oman and instead matched a block page issued by India's Department of Telecommunications. Filtered websites with this block page included multimedia sharing sites dedicated to Indian culture and entertainment. Furthermore, Omantel has a traffic peering arrangement with India-based ISP Bharti Airtel ASNs AS8529 and AS9498, and trace routes of attempts to access the blocked content from Oman confirmed the traffic passed through Bharti Airtel. We found that the filtering resulted from a broad Indian court decision that sought to limit the distribution of a recently released film.

Omani users were thus subject to filtering implemented for domestic purposes within India. These users had limited means of accessing content that might not have violated Omani regulations, did not consent to the blocking, and had little recourse for challenging the censorship.

Collateral Filtering

ISPs often implement Internet filtering in ways that can unintentionally block content. Ineffectively applied filtering can inadvertently block access to an entire domain even when the censor was targeting only a single URL. IP blocking can restrict access to thousands of websites hosted on a single server when only one was targeted.

Commercial filtering lists that miscategorize websites can restrict access to those that do not contain the type of content censors might want to block. We refer to such over-blocking as "collateral filtering" -- the inadvertent blocking of content that is a by-product of crude or ineffectively applied filtering systems.

The idea of collateral filtering implies that some content is blocked because censors target it, while other content is filtered as a side effect. However, the distinction between these two content categories is rarely self-evident from technical data alone. We must understand what type of content censors are trying to block — a challenging determination that requires knowledge of the domestic political and social context.

Collateral filtering can occur from keyword blocking, in which censors block content containing particular keywords regardless of context. Our research in Syria demonstrated such blocking's effects, and illustrated how we can redefine testing methods if we understand the censoring regime's targets. Syrian authorities have acknowledged targeting Israeli websites, letting us focus research on enumerating this filtering's depth and breadth. Past research has also documented the country's extensive filtering of censorship circumvention tools. Data gathered from Syria has demonstrated that all content tested that contained the keywords "Israel" or "proxy" in the URL was blocked, a crude filtering method that likely resulted in significant collateral filtering.

Similarly, our research in Yemen has indicated that the ISP YemenNet blocks access to all websites with the .il domain suffix, such as Israeli government and defense forces websites. However, several seemingly innocuous sites also ended up blocked, including that of an Italian airline selling flights to Israel, and that of an Israeli yoga studio. This content was filtered using non-transparent methods, in contrast to the transparent methods used to filter other social content

While technical data identifies which content is filtered in cases like Syria and Yemen, it cannot tell us if the content was intentionally targeted or is filtered as a byproduct of how that censorship is applied. Contextual information that clarifies the issues and groups relevant to censoring authorities provides a framework around which technical interrogation can be structured. In these circumstances, the technical data and contextual information complement each other iteratively, as testing methods can be informed and refined by a deeper understanding of the censor's motivations.

Methodological Challenges

Using a mixed-methods approach to study information controls can help us pinpoint which technical measurements to use and add valuable context for interpreting the intent of a regime. However, challenges remain. In our work, we have wrestled with perennial difficulties in data collection, analysis, and interpretation that are general challenges for multidisciplinary research on information controls.

Any Internet censorship measurement study will encounter the seemingly simple but actually complicated questions of determining what content to test, which networks to access, and when to target testing.

Determining what content to use to test Internet filtering is challenging in terms of both creating and maintaining content lists over time. Keeping lists current, testing relevant content, and avoiding deprecated URLs is a logistical challenge when testing in more than 70 countries over 10 years. To create and maintain these lists, the ONI relies on a large network of researchers who with a range of regional expertise. Also, although keeping testing lists responsive to environmental changes increases the relevancy of their content, it can complicate efforts to measure a consistent dataset across time and countries and, consequently, can make fine-grained longitudinal analysis difficult

Network access points can be accessed in various ways, including remote access (such as public proxies), distributed infrastructures (for example, PlanetLab), or client-based approaches.
Each of these methods has benefits and limitations. Public proxies and PlanetLab enable continuous automated measurements, but are limited with regard to which countries are available or might not represent an average connection in a country, possibly introducing bias. Client-based testing can ensure a representative connection, but users may not be available in countries of interest or may not be able to access a particular ISP. In some cases the potential safety risks to users is substantial; ethical and legal considerations may restrict testing.

Our testing method relies heavily on users for testing and human analysts for compiling testing lists and reviewing results. These conditions make continuous testing infeasible and require that we identify ad hoc triggers for targeting tests. Clearly, sensitive events are potentially good indicators of when information controls might be enacted. However, as our BBC study showed, predicting which events will trigger controls is never straightforward.

A holistic view of information controls combines technical and contextual data and iterative analysis. However, this analysis is often constrained by data availability. In some cases, technical

data clearly showing a blocking event or other control might not be easily paired with contextual data that reveals the intentions and motivations of the authorities implementing it.
Policies regarding information controls might be kept secret, and the public justification for controls can run counter to empirical data on their operation. Contextual anecdotes about controls derived from interviews, media reports, or document leaks, on the other hand, can be difficult to verify with technical data due to access restrictions.

Conclusion

The study of information controls is becoming an increasingly challenging but important area as states ramp up cyber security and related policies. As controls increase in prevalence and include more sophisticated and at times even offensive measures, the need for multidisciplinary research into their practice and impact is vital. Disciplinary divides continue to hinder progress. In the social sciences, incentives for adopting technical methods relevant to information controls are low. Although the study of technology's social impact is more deeply entrenched in technical sub-disciplines such as social informatics and human-computer interaction, these fields are less literate in social science theories that can help explain information control dynamics.[20] We have tried to overcome disciplinary divides through large collaborative projects. However, collaborative research is costly, time-consuming, and administratively complex, particularly if researchers in multiple national locations are involved.

Addressing these divides will require a concentrated effort from technical and social science communities. Earlier education in theories and methods from disparate fields could provide students with deeper skill sets and the ability to communicate across disciplines. Researchers from technical and social sciences working on information control research should stand as a community and demonstrate the need for funding opportunities, publication venues, workshops, and conferences that encourage multidisciplinary collaborations and knowledge sharing in the area. Through education and dialogue, the study of information controls can mature and hopefully have greater effects on the Internet's future direction.

Acknowledgements

We thank Hal Roberts, Steven Murdoch, Phillipa Gill, and the Internet Computing reviewers for comments. We would like to especially thank the numerous collaborators and testers involved in the OpenNet Initiative over the past 10 years. The OpenNet Initiative is financially supported by the John D. and Catherine T. MacArthur Foundation.

References

[1] OpenNet Initiative, "Global Internet Filtering in 2012 at a Glance," https://opennet.net/blog/2012/04/global-internet-filtering-2012-glance

[2] For example: Anonymous. The collateral damage of internet censorship by dns injection. ACM SIGCOMM Computer Communication Review, 42(3), 2012; R. Clayton, S. Murdoch, and R. Watson. Ignoring the great Firewall of china. In Privacy Enhancing Technologies, pages 20-35. Springer, 2006, http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf; J. Crandall, D. Zinn, M. Byrd, E. Barr, and R. East. Conceptdoppler: a weather tracker for internet censorship. In 14th ACM Conference on Computer and Communications Security, pages 1-4, 2007; http://www.conceptdoppler.org; X. Xu, Z. Mao, and J. Halderman. Internet censorship in china: Where does the filtering occur? In Passive and Active Measurement, pages 133-142. Springer, 2011, http://web.eecs.umich.edu/~zmao/Papers/china-censorship-pam11.pdf.

[3] A. Sfakianakis, E. Athanasopoulos, S. Ioannidis, "CensMon: A Web Censorship Monitor, USENIX Free and Open Communication on the Internet (FOCI) 2011,http://static.usenix.org/event/foci11/tech/final_files/Sfakianakis.pdf; J. Verkamp and M. Gupta. Inferring mechanics of web censorship around the world. USENIX Free and Open Communication on the Internet (FOCI) 2012, https://www.usenix.org/conference/foci12/inferring-mechanics-web-censorship-around-world.

[4] For an example of the work of OpenNet Eurasia see: OpenNet Initiative, "Commonwealth of Independent States Overview," http://opennet.net/regions/commonwealth-independent-states-cis

[5] J. Zittrain and B. Edelman, "Empirical analysis of Internet filtering in China," 2003, Internet Computing, http://cyber.law.harvard.edu/filtering/china/; N. Villeneuve, "Project C (r.1.0)," The Citizen Lab, http://homes.chass.utoronto.ca/~citizenl/assets/articles/ProjectC-r1.pdf.

[6] J. Wright, T. de Souza, I. Brown, "Fine-Grained Censorship Mapping Information Sources, Legality and Ethics," USENIX Free and Open Communication on the Internet (FOCI) 2011, http://static.usenix.org/event/foci11/tech/final_files/Wright.pdf. For a general discussion of ethics and Internet research see: R. Deibert and M. Crete-Nishihata, "Blurred Boundaries: Probing the Ethics of Cyberspace Research". Review of Policy Research, 28, 5 (September 2011), pp. 531-537. http://onlinelibrary.wiley.com/doi/10.1111/j.1541-1338.2011.00521.x/pdf

[7] M. Crete-Nishihata, and J.C. York, "Egypt's Internet Blackout: Extreme Example of Just-in-time Blocking," January 28, 2011, https://opennet.net/blog/2011/01/egypt%E2%80%99s-internet-blackout-extreme-example-just-time-blocking

[8] A. Dainotti, C. Squarcella, E. Aben, K. Claffy, M. Chiesa, M. Russo, A. Pescape, “Analysis of country-wide Internet outrages caused by censorship,” IMC 2011, http://www.caida.org/publications/papers/2011/outages_censorship/outages_censorship.pdf

[9] OpenNet Initiative, “The Internet and elections: The 2006 presidential election in Belarus,” 2006, http://opennet.net/sites/opennet.net/files/ONI_Belarus_Country_Study.pdf

[10] Canada Centre for Global Security Studies, “Casting a wider net: Lessons learned in delivering BBC content on the censored Internet,” October 11, 2011, http://munkschool.utoronto.ca/downloads/casting.pdf

[11] N. Aase, J. Crandall, A. Diaz, J. Knockel, J.O. Molinero, J. Saia, D. Wallach, and T. Zhu. “Whiskey, Weed, and Wukan on the World Wide Web” USENIX Free and Open Communication on the Internet (FOCI) 2012, https://www.usenix.org/system/files/conference/foci12/foci12-final17.pdf

[12] OpenNet Initiative, “Yemen,” 2009, http://opennet.net/research/profiles/yemen

[13] OpenNet Initiative, “Vietnam,” http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-vietnam.pdf

[14] OpenNet Initiative, “Ethiopia,” http://opennet.net/research/profiles/ethiopia

[15] See N. Villeneuve, “The Filtering Matrix..,” First Monday, Volume 11, Number 2, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1307/1227

[16] OpenNet Initiative, “Internet filtering in Uzbekistan in 2006-2007,” 2007, http://opennet.net/studies/uzbekistan2007

[17] H. Noman, “Dubai free zone no longer has filter-free Internet access,” OpenNet Initiative, April 18, 2008, http://opennet.net/blog/2008/04/dubai-free-zone-no-longer-has-filter-free-internet-access

[18] OpenNet Initiative, “Commonwealth of Independent States Overview,” http://opennet.net/regions/commonwealth-independent-states-cis

[19] Citizen Lab, “Routing gone wild: Documenting upstream filtering in Oman via India,” 2012, https://citizenlab.org/2012/07/routing-gone-wild/

[20] For an example of International Relations theory applied to information control dynamics see:
R. Deibert. and M. Crete-Nishihata. “Global Governance and the Spread of Cyberspace Controls,” in Global Governance: A Review of Multilateralism and International Organizations, Volume 18, Number. 3, pp. 339-361 (July-September 2012). http://citizenlab.org/cybernorms2012/governance.pdf