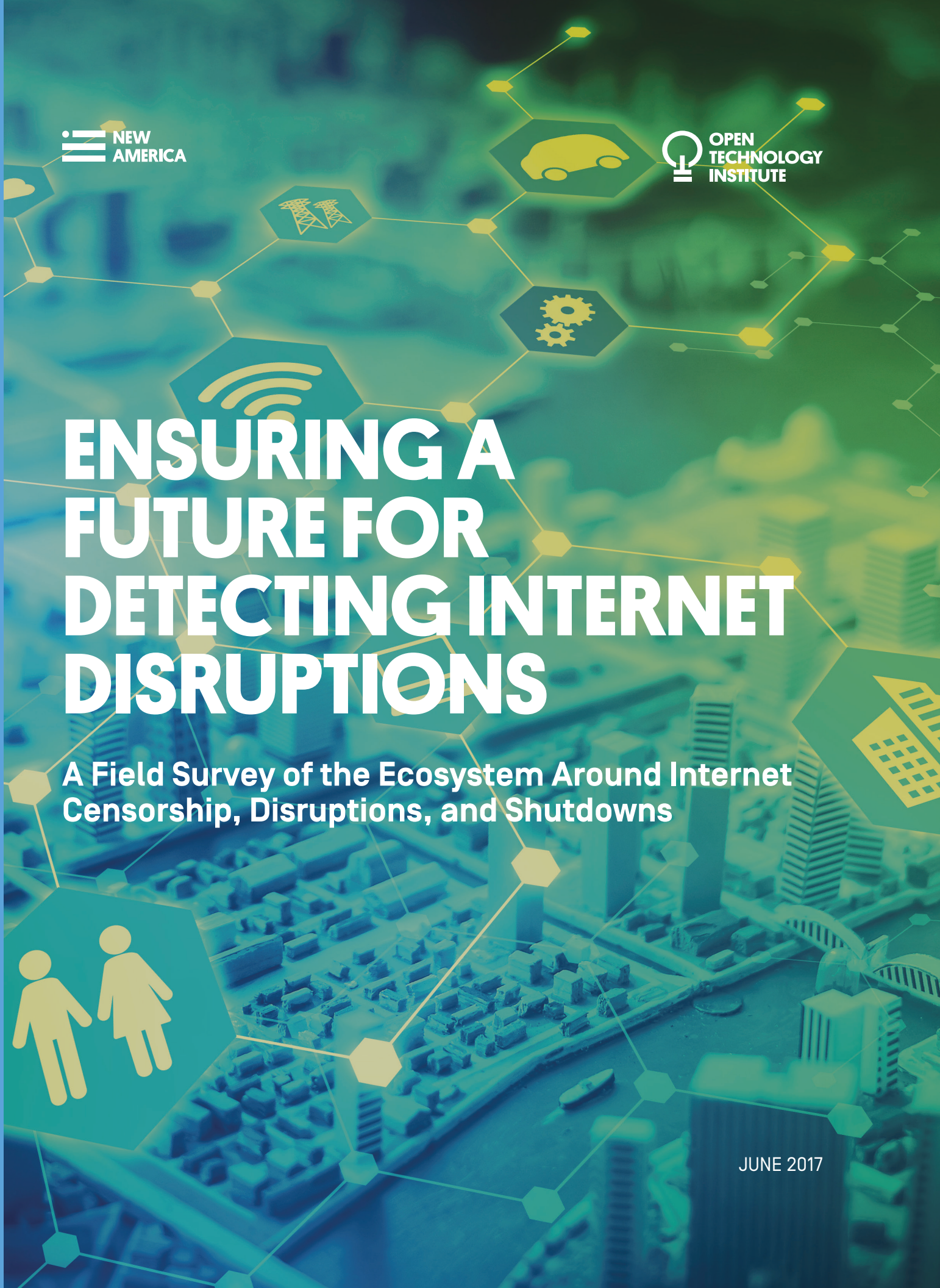


ENSURING A FUTURE FOR DETECTING INTERNET DISRUPTIONS

A Field Survey of the Ecosystem Around Internet Censorship, Disruptions, and Shutdowns

JUNE 2017

Acknowledgements

Thank you to the following for their contributions to this work: Collin Anderson, Seamus Tuohy, Liz Woolery, Georgia Bullen, and Enrique Piracés.

Thank you also to the members of the internet measurement community who took the time to participate in this research.

About New America

New America is committed to renewing American politics, prosperity, and purpose in the Digital Age. We generate big ideas, bridge the gap between technology and policy, and curate broad public conversation. We combine the best of a policy research institute, technology laboratory, public forum, media platform, and a venture capital fund for ideas. We are a distinctive community of thinkers, writers, researchers, technologists, and community activists who believe deeply in the possibility of American renewal.

Find out more at **newamerica.org/our-story**.

About OTI

The Open Technology Institute (OTI) works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

Find out more at **www.newamerica.org/oti**.

Contents

EXECUTIVE SUMMARY

When it comes to the internet, we live in a world of contradictions. While global internet connectivity is skyrocketing, governments are increasingly attempting to control their citizens' access to the internet, by enacting policies and investing in infrastructure that gives them the ability to restrict the information that their citizens can access online. In recent years, researchers, journalists, and civil society have documented an increase in global internet censorship. Attempts to curtail the free flow of information can be sophisticated or blunt, and have included the shutdown of telecommunications networks in targeted regions for extended periods of time. In response to these examples of government information control, diverse groups of stakeholders are coming together to advocate against disruptions. Recent examples of network shutdowns in several African countries during elections and periods of political unrest have shown that network measurement data can be an important tool to demonstrate harm to a broad audience, including to other governments and international organizations.

Measurement of internet censorship began in the academic computer science field well over a decade ago, starting with the study of nascent filtering systems such as China's Great Firewall. These efforts matured in scope and technical design over time, and branched out to include new areas of expertise, including social scientists and country-specific experts. There is now an active community of researchers that study internet censorship, developing software and publishing papers on the structure of filtering systems. These studies are limited in their scope because of the narrow community of funders and institutions that fund this work. As a result, researchers have prioritized tool creation and fixed-term research projects, rather than platform maintenance and long-term data collection. Until recently, those supporting the measurement community have not required or rewarded collaboration with organizations outside of the technical community.

Developing an internet measurement community that can create, sustain, and explain data-heavy outputs focused on highlighting and stopping internet shutdowns will require more formal and sustained efforts to collect internet measurements. Socioeconomic research and advocacy efforts that focus on internet shutdowns remain partially constrained by incomplete information. There is still no common understanding of what sites or applications are blocked across the world, nor any historical or real time accounts of disruptions. Measurement initiatives will have to broaden the geographic and infrastructural diversity of their data collection, and expand to cover more aspects of internet use. Moreover, recent interventions have shown that data collected by researchers outside of the censorship measurement field can play a central role in describing disruptions, necessitating

a multi-stakeholder effort that protects for sensitive data sources. To effect policy change, non-technical experts will need defensible data that can be presented in a factual manner without requiring intimate knowledge of the technical nuances of network measurement or the underlying datasets. Taken together, the next generation of measurement initiatives will require substantial financial investment and structured coordination among all stakeholders.

In order to document the state of measurement-based research on internet censorship and disruptions, OTI conducted a series of interviews with a number of key stakeholders. This paper is intended to provide a brief overview of current efforts in the censorship measurement community and focuses on recommendations to support the availability and accessibility of data on internet censorship. Primarily, we recommend the creation of:

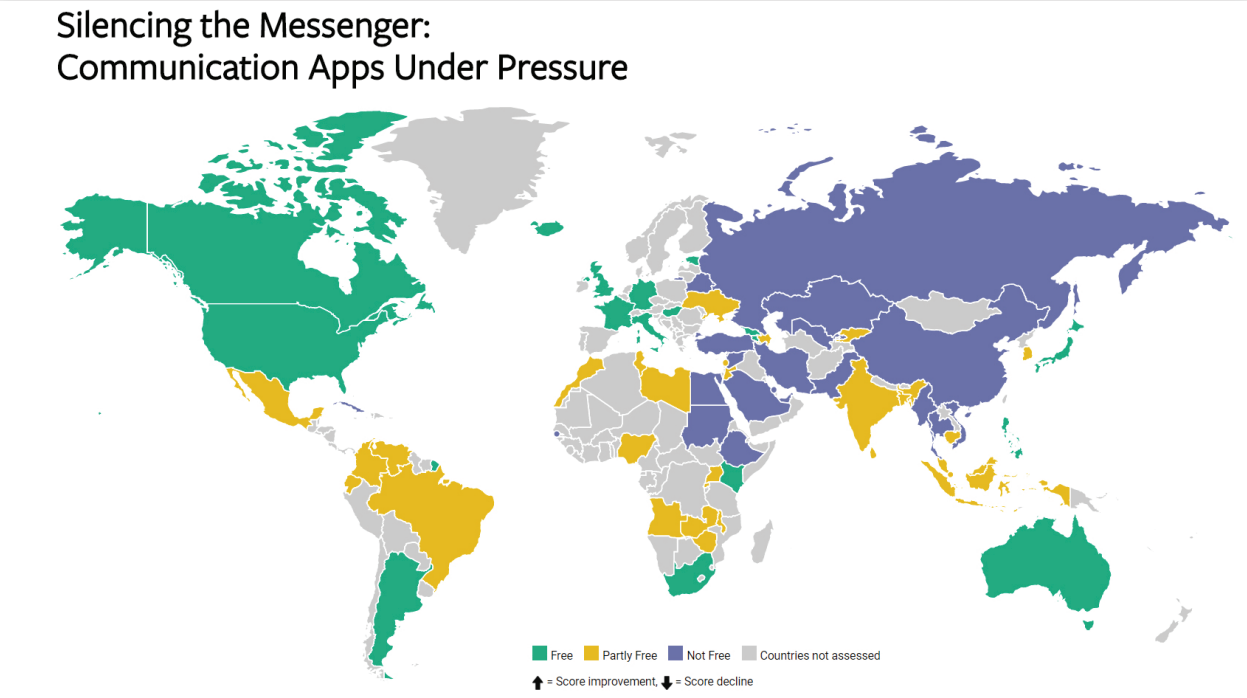
- Collaborative structures for data-sharing and coordination;
- Processes that allow the sharing of private-sector datasets and proprietary information within trusted communities;
- Funding and resources for long-term maintenance of measurement systems, and targeted support for rapid response interventions; and,
- Shared resources for comparison and presentation of measurement data.

Building a more inclusive and responsive community will be a slow process, and will require facilitation through trusted, independent entities. As a result, a cross-platform dashboard on the internet, mentioned in many of our interviews as the ideal tool for the community, is still a distant ambition. These recommendations are targeted, medium-term actions that will incrementally build professional practices and structures around collaboration. A strong, collaborative community of censorship measurement researchers, developers, and non-technical stakeholders will help to document all abuses of government censorship and improve people's ability to access the internet around the world.

INTRODUCTION

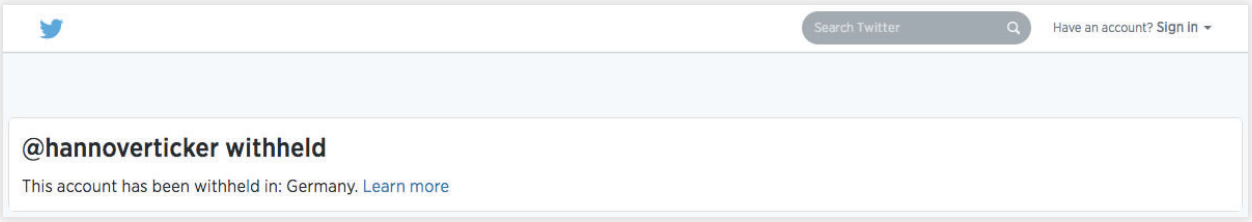
Today, two-thirds of the world's internet[1] users live in countries where content that challenges political regimes, social conventions, or national security is subject to censorship.[2] Over time, internet censorship has expanded from restricting access to IP addresses and domain names for websites, to blocking applications and persecuting users for their online activities.[3] In addition to an already diverse portfolio of techniques, governments are increasingly engaging in the complete shutdown of the internet or telecommunication services within their borders.[4] Governments now have the ability to

Figure 1 | Freedom House Freedom on the Net Map



Freedom House, Freedom on the Net 2016, Silencing the Messenger: Communication Apps Under Pressure, 2016, https://freedomhouse.org/report/freedom-net/freedom-net-2016.

Figure 2 | Blocked Twitter Account



Ranking Digital Rights. 2015 Corporate Accountability Index. (Ranking Digital Rights. 2015), 25.
https://rankingdigitalrights.org/index2015/assets/static/download/RDRindex2015report.pdf

apply shutdowns and other restrictions in a more targeted manner, and authorities commonly cut off specific regions in response to local instability, dissent, or insecurity. As more governments place onerous restrictions to prevent the free flow of information, and directly contradict widely-accepted international commitments on human rights such as the Universal Declaration of Human Rights, there is an even greater need to shine a bright light on these practices. This report offers an overview of the state of censorship measurement research in order to provide recommendations that would make rigorous measurement data more available to interested stakeholders, all in service to the ultimate goal of protecting and promoting internet freedom around the world.[5]

Governments have been able to engage in censorship and disruption without repercussions because these practices have been opaque to the international community and incongruently documented with incomplete evidence. In the past decade there has been increasing civil society engagement and advocacy in order to curtail interference and impose costs on violations of digital rights.[6] In addition to human rights NGOs, a diverse coalition of stakeholders from different communities have become involved in documenting and advocating around internet freedom, such as academia, the private-sector, media, international organizations, and other governments. This community has been particularly focused on preventing the shutdown of networks and interference with applications or websites. The public face of advocacy belies the broad interests at stake. While private-sector organizations and governments typically do not engage in public advocacy, they have natural interests in the prevention of interference and play an important role that is relevant to the measurement ecosystems.[7]

For these stakeholders, censorship measurement is a means to an end. By developing better tools and providing robust data sets that are accessible, open, and usable, censorship measurement efforts could allow non-technical stakeholders to more easily substantiate claims of internet censorship and empower a range of actors to more effectively challenge abusive practices. The same effort would allow social scientists and economists to produce rigorous cross-disciplinary research on the impact and trends of internet censorship.[8] The potential benefits of increased data can be seen in recent efforts to quantify the financial impact of internet shutdowns, which provided civil society and companies with the opportunity to ground their arguments in economic development terms and to involve new parties such as international finance institutions.[9] Collectively addressing repressive blocking and shutdowns will require a collaborative relationship between the technical community, the private-sector, civil society, international organizations, and other stakeholders.

In order to outline a path forward, it is crucial to start by understanding the current state of the community and its unaddressed needs. Over the course of several months, beginning in October 2016, New America's Open Technology Institute

(OTI) conducted a series of in-depth interviews with representatives from within the internet freedom and censorship measurement communities. Interviewees covered a broad cross-section of stakeholders, including tool developers, tool users, online platform creators, researchers, NGO employees, foundation staff, and funders. The sessions were semi-structured, beginning with a foundational set of questions shared across all interviews. The interviews touched on several main themes: awareness of tools, motivations, use of tools, ideal capabilities, the terminology used to discuss this work, existing data sources, potential data sources, and more (example questions are included in Appendix IV).

Based on interviews, we have identified core areas where efforts to document shutdowns and censorship have been successful, and where there remain unaddressed needs. Across this report, we seek to:

- Characterize the themes of efforts to measure and advocate regarding censorious interference with the free flow of information over the internet;
- Enumerate common challenges posed to the measurement community; and,
- Document the outstanding needs of existing measurement initiatives, the structural impediments to their success, and the differences that exist among them.

Through the assessment project described above, we developed a series of recommendations that support a more comprehensive and effective censorship measurement community. Documentation and information produced during the interviews on the themes of responses, product of research, and attempts to categorize efforts can be found in the Appendices.

Case Study: December 2016 Gambia Election

On December 1, 2016, Gambian President Yahya Jammeh was defeated in reelection, ultimately ending a twenty-two year tenure marked by rampant human rights abuses.[10] The electoral loss was preceded by large-scale protests in opposition to the president, prompting a crisis that would escalate after Jammeh refused to concede power. The Gambian election also marked the latest incident in a nascent regional trend: the shutdown of telecommunications networks and blocking of internet services in response to political instability.

The Gambian blackout was of no surprise to human rights advocates; recent post-election violence in Gabon was met with an internet shutdown and at least ten other African Union member countries had previously restricted networks to assert political control.[11] Anticipating problems, a community of regional and international NGOs organized under the Access Now led "#KeepItOn" campaign wrote an open letter to Jammeh urging the president not to disconnect the internet. Meanwhile, the censorship detection platform OONI, the Open Observatory of Network Interference, coordinated with a local NGO to host a measurement probe inside the country. As feared, late in the evening before the election, Gambia began to fall off the global internet.[12]

OONI faced a peculiar problem: if internet access was disconnected, how could its probe communicate back to its operators to provide data? Fortunately, the Gambia disconnection was not subtle, as no country can entirely disconnect from the internet without leaving fingerprints behind. The withdrawal of the Gambian networks from the internet was widely visible within publicly-available internet routing data. Any user with access to the right tools could watch as Gambia pulled the plug. Moreover, those monitoring internet platforms and services watched as the number of users from Gambia rapidly and unnaturally decreased. One

of the first companies to publish data showing a dramatic drop in traffic was the censorship circumvention service Psiphon. Within a couple of days, the content distribution networks Akamai and Cloudflare published their own observations on Twitter and their blog, respectively, followed by the automatic (but delayed) disclosure provided by Tor's metrics page.[13]

In this scenario, where an authoritarian leader was willing to exercise violence to stave off an unfavorable electoral outcome, human rights NGOs had little opportunity to directly influence the decisions of Gambia's government.[14] However, global internet freedom advocates were able to effectively push out messages to the international media and prompt foreign governments to respond to the disconnection. Several international media outlets covered the shutdown, prompted by outreach from civil society organizations using the shutdown as evidence of the repressiveness of the regime.[15] The State Department expressed its concerns about interference with internet access in a briefing on the day of the election.[16] After two days, the shutdown shifted to a "curfew" and soon after internet access was completely restored despite continued protests and instability. Given the broad range of cooperation and preparation efforts between diverse communities, the Gambia case is an important milestone in the coordination of data-driven advocacy to end the practice of internet shutdowns.[17] Subsequent cases demonstrate the importance of data and advocacy around shutdowns, as those campaigns, such as one targeting a protracted regional shutdown in Anglophone Cameroon, resulted in challenges from members of the European Parliament on continued foreign aid and other international responses.[18]

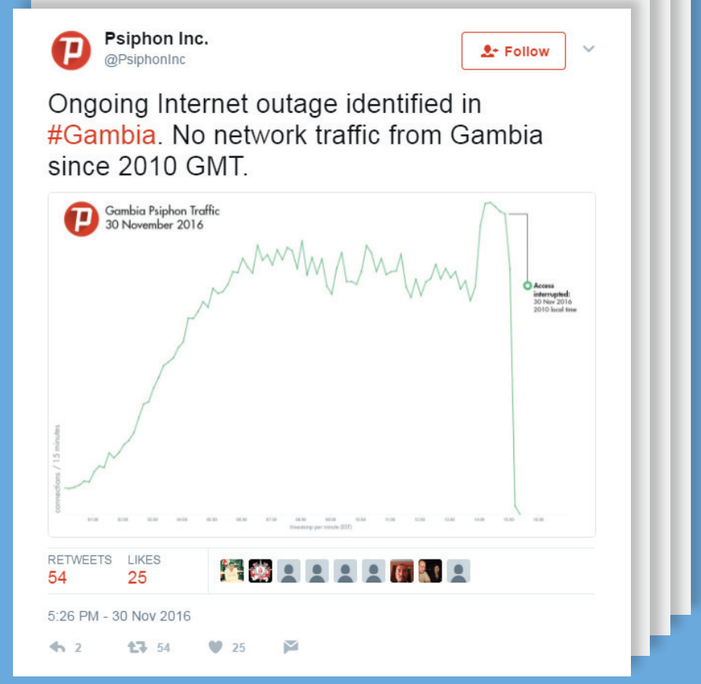
> **OONI faced a peculiar problem: if internet access was disconnected, how could its probe communicate back to its operators to provide data? Fortunately, the Gambia disconnection was not subtle, as no country can entirely disconnect from the internet without leaving fingerprints behind.**

DOCUMENTING THE 2016 GAMBIAN INTERNET SHUTDOWN

(Figure 3)

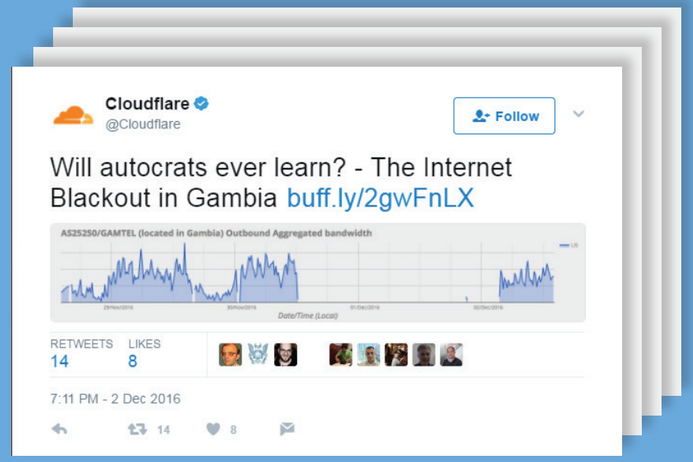
RIPE NCC, Country Routing Statistics (Gambia). **https://stat.ripe.net/widget/country-routing-stats#w.resource=gm&w.zoom_start=1480042800000&w.zoom_end=1481079600000&w.comparison=no**

(Figure 4)



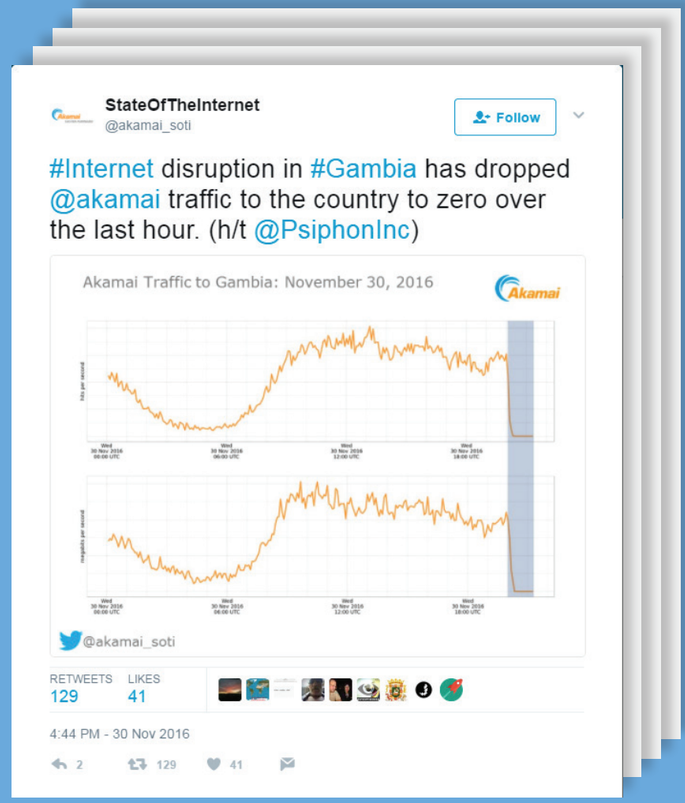
Psiphon, @PsiphonInc, November 30, 2016, 5:26 pm. **https://twitter.com/PsiphonInc/status/804089275017023488**

(Figure 6)



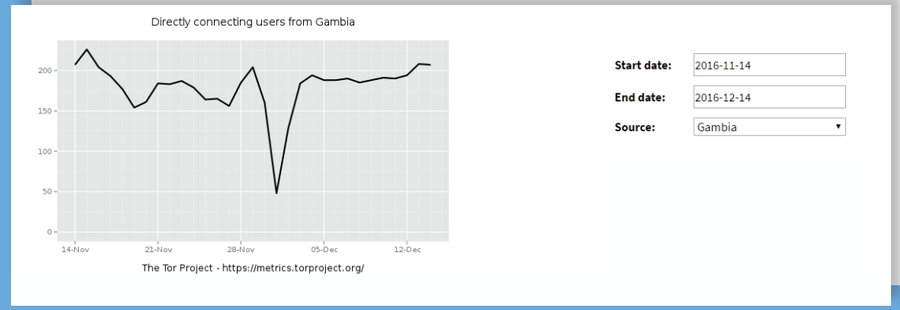
Cloudflare, @cloudflare, December 2, 2016, 7:11 pm. **https://twitter.com/Cloudflare/status/804840532245671936**

(Figure 5)



Akamai, @akamai_soti, November 30, 2016, 4:44 pm. **https://twitter.com/akamai_soti/status/804078632222294016?lang=en**

(Figure 7)



Tor Metrics, "Directly Connecting Users from Gambia," November 14, 2016 - December 14, 2016. **https://metrics.torproject.org/userstats-relay-country.html?start=2016-11-14&end=2016-12-14&country=gm&events=off**

OVERVIEW OF THE STATE OF SHUTDOWN MEASUREMENT

Stakeholders

Holding governments accountable for interference with online freedom of expression and access to the internet requires a robust community of researchers and advocates that uses technical methods to rigorously document repression. The censorship measurement field is a small and relatively nascent community, and the application of measurement data to activism within politically-sensitive contexts is still rare. After years of research on the forms and instances of interference in internet access, there is still not a complete understanding of what is blocked across the world and how often networks are disrupted. There continues to be insufficient data about who controls telecommunications networks, how control is exerted, and who is impacted. None of the current efforts have been quick to produce and contextualize data that is tactically useful for advocates in rapidly-changing circumstances or comprehensive enough for global analysis. As a result, attempts to develop broad studies on international trends in internet censorship or to engage in socioeconomic analysis on the harms of interference are constrained by a dearth of robust datasets and a lack of coordination.

These data collection strategies can be improved by the research originating within the technical community. For over a decade, computer scientists have used measurement data to conduct structural analysis of internet censorship regimes for academic publication.[19] These research initiatives have been built on one another over time, and are increasingly engaged with external stakeholders to broaden their scope and collect richer datasets. It is now more common for computer scientists in academic institutions to collaborate with international and local civil society organizations to organize measurement efforts than in the past.[20] This relationship is symbiotic: in return for opportunities to productize the tools and collect data for papers, researchers facilitate data-driven advocacy based on empirical methods that would otherwise be outside the reach of civil society.

Stakeholders with divergent incentives and varying constraints account, at least in part, for the current state of the censorship measurement field. Many of the research and platforms that focus on measuring censorship have been developed in the academic computer science field, where the motivation to develop tools and collect data is based on paper publications and research grants. These funding sources and commitments primarily cover only the development of the measurement tools but do not provide support for harnessing its potential to generate on the ground impact. Without continued

financial support, the value of maintaining the tools and expanding their deployment quickly drops off after papers are published. Peer review processes significantly reduce the timely responsiveness to rapidly evolving events, such as political crises. While some projects have included external data sources in the course of producing research on particular events, collaboration between the computer science community and social scientists or local NGOs remains rare. Moreover, computer scientists are not always well positioned to enlist volunteers in countries that require negotiating unique political sensitivities and understanding of the potential risks.

In contrast to academia, civil society is motivated to collect data in order to engage in advocacy and respond to real time events. For international and local organizations on the ground, robust datasets provide documentary evidence of the violation of freedom of expression rights and inform strategies to circumvent those blocks. This technical data can support the claims made about the policies of governments or companies, and feed into assessment projects such as Ranking Digital Rights[21] and Freedom House's Freedom on the Net[22] reports. Local NGOs can engage in contextual studies with in-depth research on particular disruptions at the national level, and highlight the issue at regional and local events. However, civil society commonly does not have the in-house technical capacity to sustain tool development or implement the existing, sometimes highly technical, software systems. Similar barriers to entry also prevent journalists and other media organizations from being engaged in censorship measurement.

Private companies may be economically and operationally motivated to support the censorship measurement field in order to sustain their customers' access to their services. However, while the private sector may be cognizant about human rights or revenue impacts, most of their decision making is driven by operational considerations. They are disincentivized from cooperation based on legitimate concerns about prosecution, retaliation, or politicization.[23]

Each community brings to the table its own set of motivations, limitations, and values. By understanding these motivations, tool developers and others can incorporate these needs into their tools and create value within a broader ecosystem.

Documentation

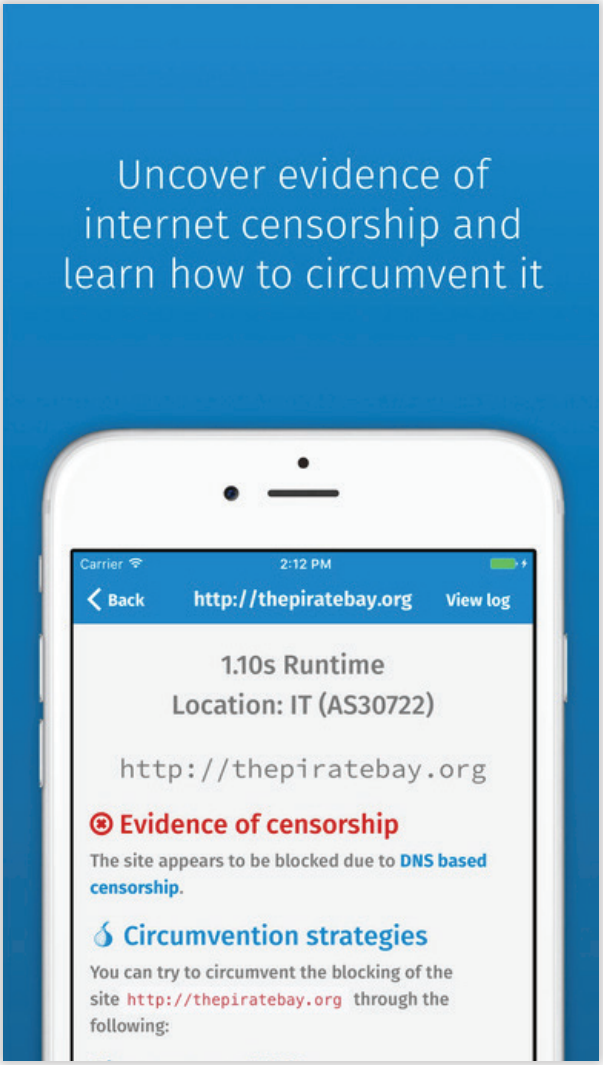
For all of these stakeholders, censorship measurement provides a shared set of insights, specifically:[24]

- Incident detection: to identify potential episodes of network interference;
- Incident analysis: to contextualize, investigate, and report additional facts related to an event;
- Trend analysis: to enable longitudinal research and macro-analysis; and,
- Response support: to provide data in support of mitigation of disruption.

As the example of Gambia illustrates, there are many stakeholders and measurement initiatives relevant to documenting shutdowns and disruption. The traditional method involves coordinating with individuals inside a country to run a software client or host a hardware probe that performs technical measurements to understand the experience from the user's connection. These platforms can be either specially-designed to collect data on censorship (such as OONI and ICLab) or general-purpose internet measurement tools (such as Measurement Lab and RIPE Atlas). Alternative approaches to measurement enlist publicly-reachable Internet infrastructure in often unintended ways to collect indicators of abnormalities or interference. These methods do not require the direct participation of users, and reduce the burden of enlisting in-country volunteers and potential user harm.[25] These measurement methods also have opportunity costs, limited to assessing a small number of metrics and provide less diagnostic information on how restrictions are implemented.

Researchers have incorporated novel sources of data beyond solely censorship measurements to understand shutdowns. The Gambia shutdown first showed up in internet routing data (BGP),

Figure 8 | OONI



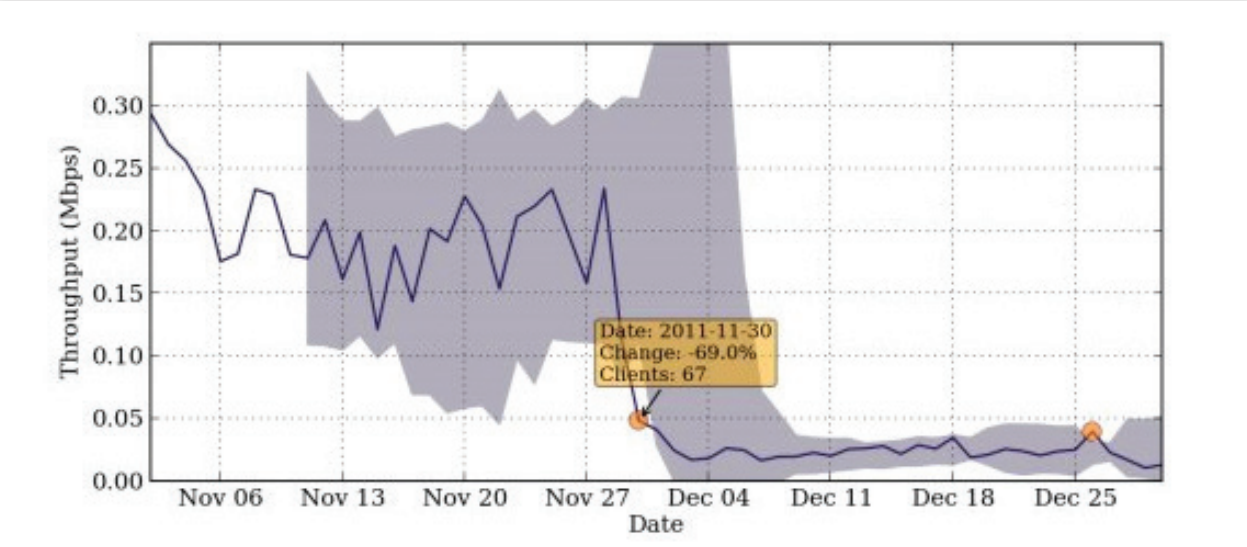
iTunes Store Preview Screenshot, Accessed June 5, 2017. http://a4.mzstatic.com/us/r30/Purple122/v4/26/21/b8/2621b82f-f8e8-02ef-7ea7-411d5168247a/screen696x696.jpeg

which is critical to the functioning of the internet and is accessible to everyone. Another passive indicator used in the Gambia case was the change in the amount of traffic directed to popular internet platforms and services. While this information is not as precise or technically rich as end-user measurements, significant drops in user counts or volume of traffic from a location (especially when spread uniformly across mobile and fixed-line traffic) can suggest a disruption. Some platforms already provide this data (e.g. Google's Transparency Report) or have demonstrated a willingness to do so for specific incidents (e.g. Psiphon). Researchers commonly propose innovative approaches to collect data from new resources. CAIDA's Internet Background Radiation (IBR) project presents a robust alternative to relying on commercial services, by using malware sinkholes and other internet artifacts that are unlikely to be blocked or constrained by the ethical concerns associated with active testing.[26]

Ethics and Research Considerations

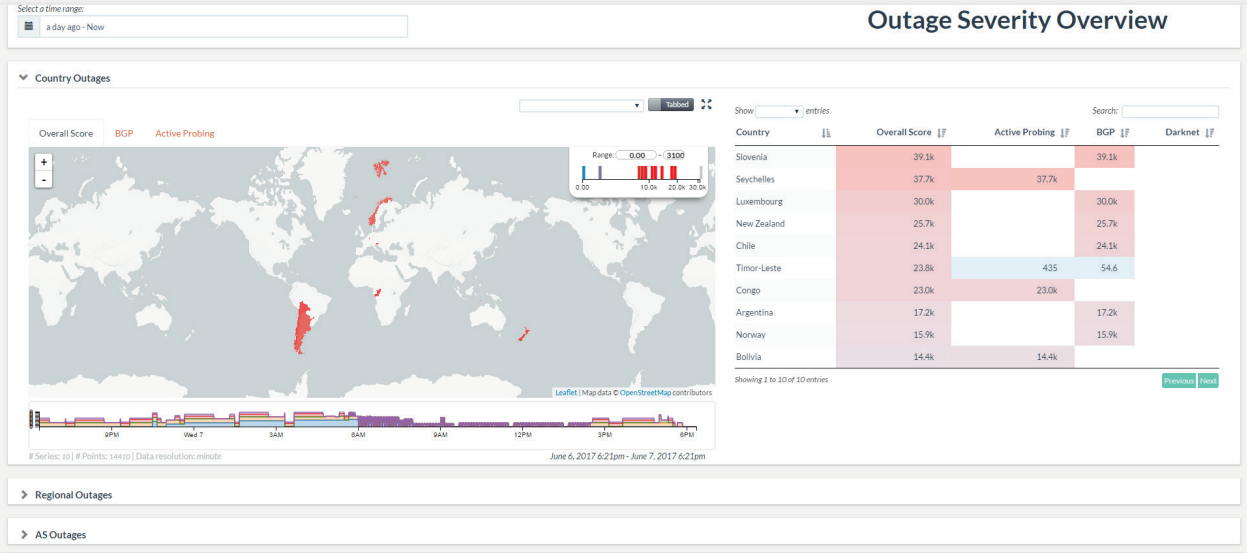
All measurement initiatives face technical, legal, and ethical constraints that limit opportunities to conduct specific experiments or share certain data. Data collection and disclosure choices involve the consideration of user risk. The types of governments that interfere with internet access for political purposes often also persecute individuals who cooperate with foreign organizations or work on human rights.[27] In order to help participants make informed choices about the potential risks of cooperating with this research, those conducting censorship measurement projects should be familiar with the applicable laws and be transparent about potential repercussions.[28] It is challenging for researchers and users alike to fully account for political and legal contexts to adequately communicate risk, especially in countries where the rule of law is weak. There are basic steps that many projects have taken to address these ethical concerns: censorship measurement platforms typically do not collect personally-identifiable information, such as the IP address of the client, and some do not release raw data at all. These circumstances have a meaningful impact on the design and operation of measurement platforms,

Figure 9 | Speed Throttling As Detected by Measurement Lab



Collin Anderson, Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran, (arXiv:1306.4361 [cs.NI]), June 18, 2013. https://arxiv.org/abs/1306.4361.

Figure 10 | IBR Dashboard



Center for Applied Internet Data Analysis (CAIDA), "IODA Outage Severity Overview," June 6, 2017. https://ioda.caida.org/ioda/dashboard

and of the types of information they can provide on censorship events (more on these factors is included in Appendix I).

As the forms of interference change, so too must the measurement systems. For much of the history of academic and NGO community research in this field, analysis on filtering regimes has tended to treat countries as homogenous entities, and therefore derived lessons from measurements conducted from a sole vantage point. However, shutdowns and disruptions no longer have to be whole-scale disconnections from the internet for an entire country. There are several cases of interference that were limited based on geography, or more subtle degradation than a full-scale shutdown. For example, rather than disconnect, Iran and Bahrain have throttled speeds in order to limit access.[29] Measurement systems and data providers also need to account for regional disruptions, such as those that have occurred in Kazakhstan, Pakistan, Cameroon, Crimea, India, China, and elsewhere.[30] Moreover, measurement tools cannot always attribute the cause of identified interference, as technical issues can appear to be blocking and not all outages are necessarily censorship.

Despite the long history of research and large number of publications on internet censorship, the field is still maturing and data remains scattered, or wholly unavailable, across different initiatives for often valid reasons. The technical methods used to restrict access to internet services, and the corresponding opportunities to measure these interventions, vary substantially, making it difficult to fully document all potential interference. As a result, there is currently no individual tool that can address every use case, nor is there likely to be one any time soon. However, there are common challenges where collaboration that can mutually enrich the initiatives and the rich set of stakeholders could contribute to the evolution of the field. By all accounts, internet censorship is only increasing, both in the number of countries blocking content and the cases of extreme interference, widening the distance between the net impact of internet censorship and our understanding of the scope of the practice.

INTRODUCTION TO RECOMMENDATIONS

When asked about the ultimate product that is needed to support better censorship measurement, stakeholders throughout the community, both within the interviews conducted for this paper and in previous statements, ask for a reliable dashboard that tracks internet censorship around the world on a real-time basis. Such a demand is deceptively complex, necessitating the measurement of connectivity from not only every country, but also from every mobile and fixed-line internet service provider in both urban and remote regions, and for every popular application and online service. There is no individual measurement tool that can address every potential form of interference, and there are many tools that are needed but are not yet built. This grand vision requires assembling and comparing data from a wide range of datasets and tools, itself a burdensome process without a straightforward solution, which requires increased collaboration and coordination between stakeholders with divergent interests.

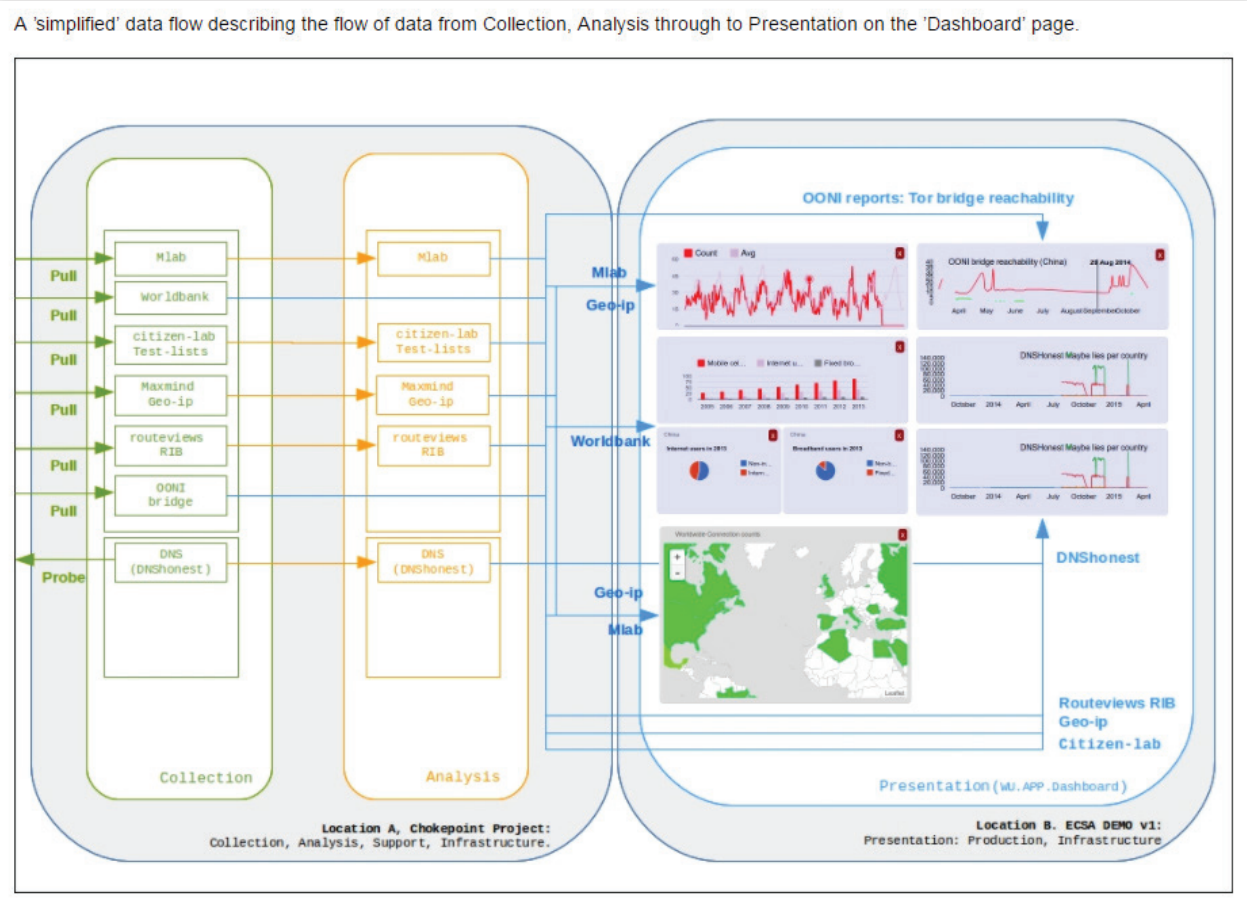
A comprehensive measurement dashboard would require the ability to present the analysis to multiple audiences with varying needs. It would have to serve the unique demands of the advocacy community, service providers, academics, and policy-makers. To do so effectively requires the creation of clear data visualizations for non-technical users that are both adaptable to different use cases and accurate as an actionable data source. This is a balancing act that is fraught with problems. Once data is collected, it requires someone to analyze and contextualize the data in a form that is accessible to non-technical audiences. Simplistic or confusing visualizations can lead to inaccurate or incomplete assertions about the data, undermining the value of technical measurements.[31] The assessment described here is the first step in delivering more comprehensive censorship measurement analysis which can promote harmonization and cross comparison.

Recognition of the limitations of purely technically focused censorship measurement efforts – those disconnected from policy and advocacy efforts – has opened a positive dialogue among stakeholders, often led by funders and researchers. The USENIX Free and Open Communications on the Internet (FOCI) workshop was formed in order to increase the cross-disciplinary collaboration involved in technical research on censorship, bringing in social scientists and local country experts.[32] In a recent grant solicitation for censorship measurement work, the State Department made clear that successful applications would be those that included a consortium of organizations, rather than one single institution.[33] Similarly, the Open Technology Fund's

(OTF) Information Controls Fellowship Program favors applications that have strong connections to at-risk communities.[34] OTF has also used its project funds to incentivize technical measurement platforms to collaborate with local organizations on a regular basis, as demonstrated in the frequent reports produced by OONI and other OTF grantees. In 2013, the European Commission's DG-CONNECT program initiated an extended study to assess the feasibility of a "European Capability for Situational Awareness" (ECSA), a mechanism to monitor cases of internet interference and provide contextual analysis of these events.[35] Google and Citizen Lab have convened spaces for measurement projects to speak about their work and collaborate on common issues, as well as a way to bring in local partner organizations.[36] These meetings have had the positive effect of increasing familiarity within the small community and resulted in some collaboration, such as shared testing lists. Still, much more can be done.

In our stakeholder interviews, there was widespread consensus that there are unfulfilled opportunities

Figure 11 | Simplified Data Flow



The Chokepoint Project, "European Capability for Situational Awareness (ECSA) DEMO v1.0 walkthrough (step 4 of 5)", https://ecsa.chokepointproject.net/walkthrough/step/4

for strategic collaboration that could benefit all those involved. Many of the historical ad-hoc attempts at collaboration have been hampered by complex challenges. Censorship measurement projects will always face roadblocks related to ethical considerations and resource scarcity. Despite these impediments, there remain ample unaddressed opportunities for independent initiatives to maintain common resources and collaborate in areas of mutual interest, such as visualization and standardizing data and processing. Overall, the interviews highlighted the need for structured spaces to facilitate collaboration across different contributor types.

In the absence of a mature and collaborative measurement community, the ambition of an all-encompassing dashboard built on coordination and disclosure of data is beyond even the medium term range of possibilities. In its own recommendations, the ECSA report noted that "it is certainly too early to implement a federation based on an automated data analysis platform as the process of data collection by potential stakeholders is mostly manual and grounded in a wide range of disciplines." Instead, the authors recommended supporting interdisciplinary research and cross-sector expertise.[37] The following recommendations focus on the creation of organizing structures and allocation of resources in ways that will facilitate more effective data-driven advocacy and accountability. These collaborations are directed at reducing the barriers to accessing data and improving the responsiveness of measurement platforms to broader community needs. Such structures will also need to include stakeholders who typically do not engage in measurement-based policy discussion, with the specific intent of facilitating data and cooperation from private sector entities that have unique and unmatched perspectives into disruptions. Increased collaboration with non-technical stakeholders will be mutually beneficial, as country-specific experts can provide the political context necessary to understand the data. Over time, these can build toward a clearinghouse focused on the collection, aggregation, enhancement, cleaning, and public presentation of network measurement data that has a sustained impact.

RECOMMENDATIONS

Foster the development of collaborative structures for data-sharing and coordination

We propose the creation of cooperative structures within the censorship measurement space that would bear responsibility for fostering much-needed collaborations to build toward concrete outputs, such as coordination between censorship measurement tools and resources. These mechanisms would promote cross-disciplinary knowledge sharing, and further facilitate collaboration between peers across their areas of specialized expertise. The need for such an initiative was expressed by many interviewees, with varied reasons ranging from protecting business interests to personal beliefs, reflecting the multitude of potential contributions and ways to promote participation.

As described across interviews, measurement initiatives offer specific value to governments, civil society, and private companies because they provide independent metrics for use in private and public advocacy. Likewise, the technical community is often ill-equipped to handle social and political hurdles outside its expertise, and has benefited from collaboration with external stakeholders. Despite these mutual needs, these stakeholders are not always in touch. The responsibilities and activities of the platform to address gaps in cooperation could potentially include:

- Managing a catalogue of data source and enabling the submission of data for community use;
- Maintaining information and common resources in a manner that ensures that data is accessible for cross comparison and analysis;
- Tracking incidents, and determining whether data exists or what would need to be developed in order to better document such events;
- Fostering the inclusion of new partners into the community and managing relationships between participants where useful; and,
- Facilitating coordination between pertinent stakeholders in order to provide timely data on incidents.

Rather than a decentralized initiative, the responsibilities of such a community will require active management from a trusted entity. The collaborate structure will need to allow various stakeholders to exchange data with confidence that the data provided will be used, protected, and shared appropriately. While certain informal mechanisms partly exist through forums like the Global Network Initiative (GNI), they are not tailored to the special requirements of the censorship measurement field and do not include many of the participants in the community, such as

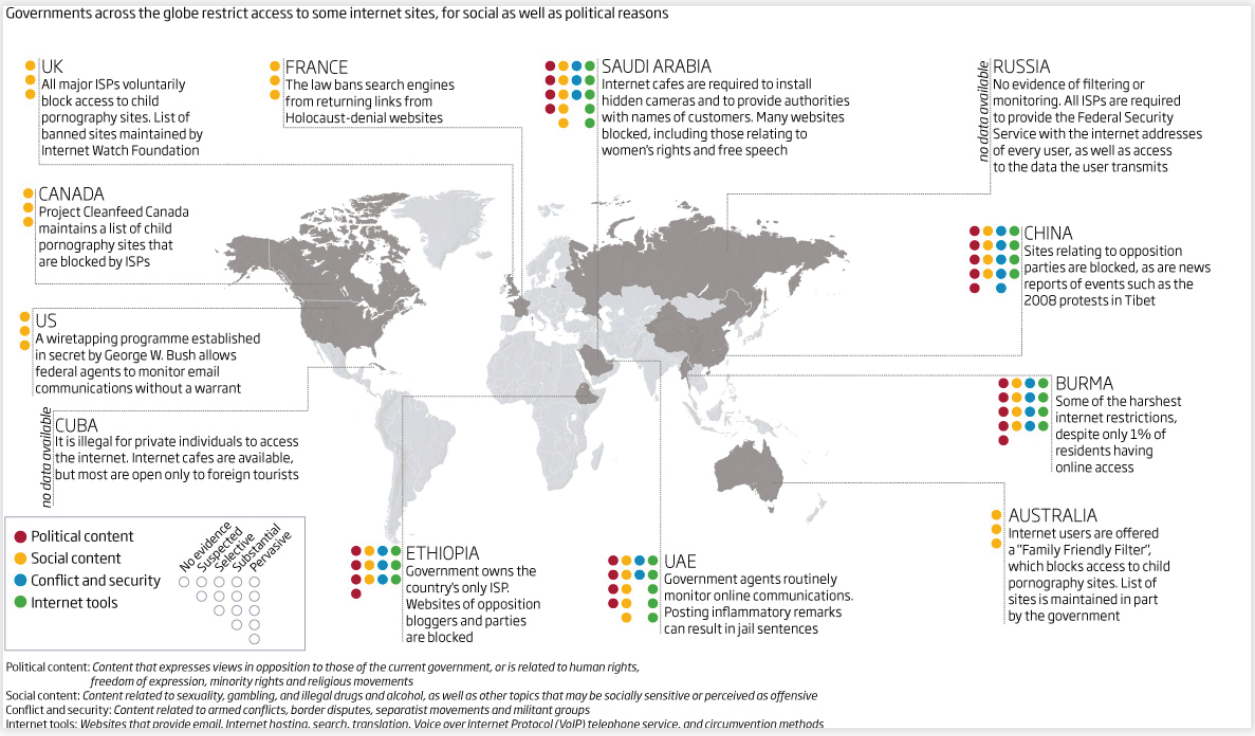
measurement tool developers. Specialized spaces could also provide a venue for technical initiatives to solicit feedback on mission critical non-technical questions, such as:

- Threats to participants and other ethical considerations;
- Strategies and partnerships to recruit volunteers to host measurement devices;
- Calendars of common censorship triggering events; and,
- Conditions within countries that are relevant to censorship measurement.

These requirements and limitations have ample parallels in other technical fields. The cybersecurity realm has fostered a series of collaborative structures for sharing threat intelligence to enable companies to collectively address threats.[38] These structures range from ad-hoc person-to-person relationships (an arrangement that is most relevant to the current censorship measurement space) to formalized information exchanges where structured data is shared across industries and groups.[39] The ECSA feasibility study is instructive on potential participatory models, data sources, data governance structures, and partners for such an initiative. These types of structures can also be found in the humanitarian data, health, civil society, and crisis response communities.[40]

A organization acting as a community maintainer could be responsible for creating an "events database" that would aggregate contextual information on each country, providing a more comprehensive view of information controls around the world. Such a database would potentially

Figure 12 | Internet Clampdown



New Scientist, "Internet Censorship on the Rise," May 27, 2007. https://www.newscientist.com/data/images/archive/2722/27224101.jpg

include information pertaining to laws, policies, and regulations that are relevant to censorship and freedom of expression, as well as information about the network landscape of each country. Furthermore, this database would aggregate information about reported cases of censorship and surveillance, enabling partners to gain a better understanding of information controls in a country and determining the appropriate tests to run. It would also enable the internet freedom community to rapidly respond to censorship events and to tailor testing accordingly.

By creating an independent collaborative structure, the community would be able to provide a common location for those seeking data and a reliable space for potential coordination. Many of the data creators and consumers that were interviewed desired more rapid and widespread data-sharing. The ability to quickly and easily access a range of different sources of data would allow analysts and advocates to create cross-verified findings and allow private-sector stakeholders to more easily identify the source of technical disruptions. Through moving from assumptions based on single-sourced indicators to allowing cross-validation across multiple data sources, the collaborative structure would improve the resiliency of data-driven activists and reduce the potential for false assertions. Furthermore, such an intermediary could enrich measurement data with third party resources, such as pertinent Google News feeds, Google Trend information, or social media reports.

Blocking and disconnection is largely driven by government actors responding to events that are country-specific and ever-shifting, requiring up-to-date contextual knowledge based on close monitoring. It is beyond the capacity of the staff of technical measurement platforms to keep track of all the potential windows of escalation for every country, even for something as simple as elections. Measurement providers noted that they have had some external sources of information on context, such as the Digital Defenders Partnership (DDP), Citizen Lab, or Access Now's Digital Security Helpline. More information and earlier notice on when events are becoming unstable would help provide more rigorous and responsive measurement.

The threat modeling necessary for ethics and risk assessments requires a two-way flow of information, and does not provide a binary answer of "safe" or "not safe." Researchers need to collaborate with those on the ground and censorship measurement experts to maintain a dialogue about what people feel they can safely do online. This dialogue can shape measurement efforts and be responsive to the concerns of users, deciding to not conduct certain tests or not include network information where the circumstances warrant caution. Some measurements platforms have stopped collection for periods of time that might be more dangerous for their partners, such as during a state of emergency. Better situational awareness would also enable more sophisticated strategies to handle tricky ethical issues through providing researchers guidance and support for keeping their local partners, customers, and measurement infrastructure safe.

> *In a dream world, we would have access to a panel of internet users around the world that we could ping every once and awhile to compare alongside the measurements that they do, such as "what can you safely do online?" and "what can you not safely do online?"*
>
> —MEASUREMENT PROVIDER

By acting as a community maintainer, a designated organization could better manage common resources such as an events database. This structure would ensure the community is prepared to conduct its work where it is most needed through maintaining this contextual information in a way that can be easily accessed and acted upon by censorship measurement projects (e.g. a calendar of elections or political anniversaries that could lead to an increase in information controls). Funders could also incentivize measurement providers

to be responsive to solicitations through the community. Another specific intervention would be to hold targeted workshops on a regular basis where researchers, civil society, and companies are encouraged to produce outcomes within confidential settings.

Facilitate Opportunities for Disclosures of Private-Sector Datasets and Information

Thoughtfully implemented initiatives to engage private-sector stakeholders and address their concerns would allow for greater collaboration and more effective monitoring of disruptions based on new resources. **We recommend the creation of a "private-sector network information clearinghouse" that will allow participants to provide data for aggregation, filtering, and publication.** Through the designation of an independent entity, the clearinghouse would establish the trust necessary to respect the confidentiality needs of each individual participant. This would allow the designation of entities that could engage in legal arrangements and non-disclosure agreements with private entities to serve as a bridge to the broader community. The coordinated facilitation of such disclosures would ensure that the final aggregated datasets are accurate, compelling, and valuable.

Companies in the technology sector collect large amounts of quantitative data in order to make their services work better, protect their infrastructure, address problems, and track their growth within global markets. As the case study of Gambia demonstrates, the data published by Psiphon, Cloudflare, and Akamai provided compelling evidence of the disruption of access to communications platforms. The data also provided a strong testament to the accuracy of data

Figure 13 | Google Transparency Data

Google. "Google Transparency Report, Fraction of Worldwide Traffic, Normalized (Pakistan/YouTube)". November 25, 2012. https://www.google.com/transparencyreport/traffic/explorer/?r=PK&l=YOUTUBE&csd=1339691400000&ced=1353879071379.

collected from other measurement platforms against potential challenges to the credibility of their results. Researchers have begun to demonstrate the value of such datasets as an automated monitoring mechanism for shutdown.[41] Company disclosures such as these are relatively rare, mostly published on a manual basis, and do not appear to be coordinated.

Private-sector stakeholders face difficult legal, ethical, and public relations problems around sharing any form of data publicly. Companies are legally constrained by privacy and consumer protection regulations that differ between jurisdictions and change frequently. Beyond the law, companies have often outlined what data will be shared and with whom in their terms of service and privacy policies, which adds further hurdles to disclosure. Accuracy in representation is also critical: one company interviewed used to have a real time monitoring page, but they had to shift to manual publication after false positive incidents caused confusion. Finally, a company must carefully weigh whether sharing certain datasets could damage their competitive edge.

Most companies are likely to take a "wait and see" approach to disclosure of such data. A more systematic analysis of existing public datasets and well-implemented coordination with an initial set of partners will catalyze further participation from other companies. Such arrangement would not need to immediately start with fine-grain platform logs. Instead versions of the clearinghouse could start with broad datasets, such as normalized traffic per country, and evolve based on needs and experience in order to find a balance between community needs and provider sensitivities.

Based on the interviews conducted with researchers and companies, we are confident that a minimum viable product version of such a clearinghouse could be created through already published data (e.g. Google's Transparency Report) and not-for-profit platforms that are not so restrictively constrained by commercial concerns. The primary role of this clearinghouse would be to act as a trusted intermediary in the aggregation and publication of datasets, allowing:

- Companies to contribute any level of information, including aggregated or sanitized datasets, pertinent to censorship or network shutdowns;

- Researchers and civil society organizations to present requests for access or information derived from private datasets;

- Stakeholders to foster a community of practice around disclosure of censorship events that can normalize their publication by companies, similar to law enforcement transparency reports; and,

- Companies to create data-sharing agreements that allow for the sharing of sensitive data under clearly-defined conditions of use.

The clearinghouse will require a dedicated host organization that bears responsibility for implementation and ensures compliance from its partners. Such an entity would have to be hosted by a non-advocacy organization and maintained in a neutral manner. The entity itself, or a technical partner, could act as an intermediary for sanitation of raw data sources for release if necessary. The clearinghouse would also need to separately maintain public and private information on incidents, such as:

> *Public:* incident background information, start date and end date of the incident, public rationale for restriction, open source technical, and related political information
>
> *Private:* sensitive technical measurements, disclosed datasets describing the incident, and confidential contextual information

Two interviewees referred to the Lumen Database (formerly, Chilling Effects) as an model of a coordinating platform that allows companies to disclose sensitive government requests without

putting the companies on the front line.[42] The Lumen Database is especially relevant to evaluating the sensitivities of censorship measurement, since the database's disclosures include information on the nature of the content being taken down, the entity making the request, and the company receiving it. The disclosure of interference could be less sensitive than the Lumen Database in practice, as information could be reported in much vaguer terms, such as "multiple companies reported an anomalous event," and allow for cross validation among peer companies where desired.

The creation of a trusted data clearinghouse and multi-stakeholder community will require a substantial investment of time in order to outline the requirements of partners, including the specifics of confidentiality arrangements. The potential provision of confidential data will also require a sustained resource to report issues and coordinate use (akin to the function of institutional review boards within academic institutions). This will require commitments for participation and funding from key partners, especially to encourage participation from other stakeholders. Once the clearinghouse is launched, a central entity would require maintenance funding to continue to facilitate discussions and further refine structures as needs change.

The clearinghouse will have an amplifying effect that extends beyond the direct benefits of its role as an intermediary focused on data. The clearinghouse will also benefit from non-technical disclosures, as other internet freedom campaigns have received early notice about rumors or legal demands from telecommunications companies, journalists, and others. Improved communication could also improve the overall accuracy of the field: as one interviewee framed the issue in discussing frustration with certain public datasets, "when you rely on external data – you have to know how the data is put together." The clearinghouse would be positioned to build tools to identify, sanitize, aggregate, and store real-time data feeds. Once partner approval has been obtained, the clearinghouse could provide public access to the aggregated real-time and historic data, as well as exploratory dashboards that help the public understand and correctly interpret the data.

Provide Resources for Long-Term Maintenance and Real-Time Analysis to Measurement Projects

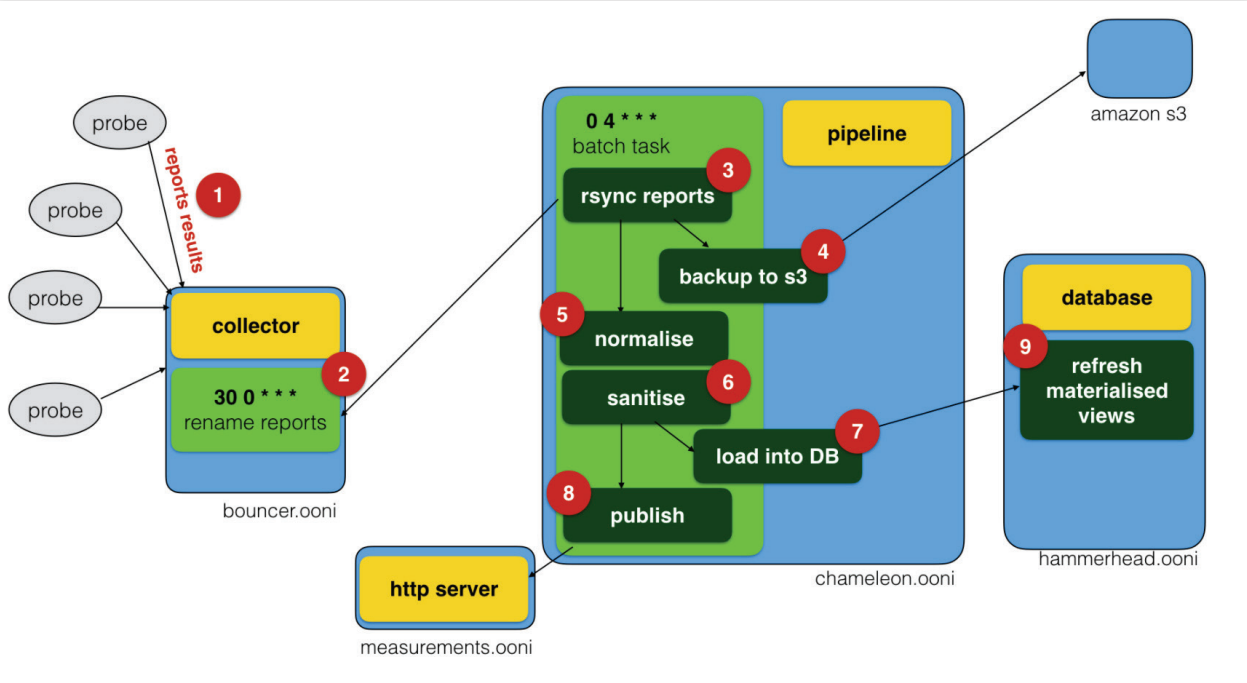
> *"Getting the news out within seconds or minutes really boosts the way the story is picked up by the press, how accurate it is picked up, and how much we can push back in response. Just getting the right methodology to get the facts right each time so we can raise awareness about the situation."*
>
> —TURKEY BLOCKS

The practical challenges related to resource constraints in the censorship measurement community should not be underestimated. There are limited resources to support both the ongoing costs of censorship measurement projects and real-time analysis of possible incidents that can bolster rapid response efforts. There are three specific areas where donors and the technology sector could contribute without duplicating efforts: 1) in-kind donations to censorship measurement projects; 2) strengthening and diversifying funding for censorship measurement; and 3) greater private-sector involvement in censorship measurement rapid response funding.

In-Kind Donations to Censorship Measurement Projects

It is important that more companies provide access to the infrastructure and expertise they have built to sustain their business services as in-kind donations to the censorship measurement community. These infrastructure donations could include the long-term hosting of historical data or computational resources for conducting measurement and data processing. They can also provide access to their in-house expertise by encouraging staff to support tool development or providing data management advice to external projects as part of their corporate social responsibility programs.

Figure 14 | OONI Storage Design



Citation: The Tor Project. "OONI Pipeline Architecture." https://raw.githubusercontent.com/TheTorProject/ooni-pipeline/21c2923c12fd1db79dfec000fbf2d05130bafc9f/docs/ooni-pipeline-architecture.png

One hidden, but substantial, cost for network measurement projects is data storage, accessibility, and searchability. Measurement collection platforms require large amounts of ongoing storage space for their results and significant computational resources to transform, analyze, and provide that data on-demand to other researchers. Current projects have attempted to address this through a variety of partnerships. Netalyzer leverages the DHS Protected Repository for the Defense of Infrastructure against Cyber Threats' data catalog;[43] Measurement Lab (M-Lab) partners with Google; RIPE runs its own infrastructure, but is facing constraints as it expands. In just one example, M-Lab has generated at least five petabytes of data, a number that is increasing at a pace of over a half-million measurements every day. Even with strong support from Google, this is a burdensome amount of data that would be difficult to sustain independently and M-Lab has struggled to make its dataset more responsive to real-time needs. Companies like Google that operate on a global scale have developed the storage space, computational resources, and expertise that the censorship measurement community sorely needs.

Many companies already have academic and researcher support programs that provide grants to researchers in the form of credits to use business-level services.[44] Providing infrastructure resources and expertise to projects would serve as a multiplier toward these existing funds. Through these types of in-kind donations, companies will be able to provide significantly greater support to censorship measurement projects at a reduced cost, and censorship measurement projects will be able to focus on the measurement instead of the management of data.

Diversified Funding for Censorship Measurement

The long-term sustainability of the censorship measurement community requires **greater diversity and stability of its funding sources.** The foreign assistance and international media programs of a few Western governments make up the largest percentage of financial contributions to the censorship measurement community.[45] We recommend that private foundations and corporate donors both establish their own funding sources and coordinate more closely with current donors.

Figure 15 | Human Rights Funding Report

International Human Rights Funders Group, "Advancing Human Rights: Update on Global Foundation Grantmaking," (The Foundation Center and the International Human Rights Funders Group, 2017), 9. http://humanrightsfunding.org/report/#page=9

This centralized financial support has made the censorship measurement community highly reliant on a few sources, predominantly from government entities, which are uniquely vulnerable to opaque budgetary decisions and changes in political climates. Private foundations can take targeted strategic risks by funding innovative projects, which government donors are prevented from making by institutional constraints around contracting and minimum contract costs. Scarcity has fostered some of the zero-sum competition and lack of coordination found between otherwise complementary projects. The lack of funding diversity has also constrained the types of issues and countries where measurement initiatives can focus their efforts, often prioritizing places where money is allocated by funders, rather than regions where small interventions are more likely to inspire better policy. Through enabling low-cost, high-risk, and high-return investments in research, private funders can enable researchers to pursue novel methods to make the measurement ecosystem more robust.[46]

The current funding environment runs contrary to needs of measurement platform operators and creates a pernicious cycle of half-developed projects. This mismatch in support versus needs weighs heavily on why successful beta projects have struggled to evolve into widescale platforms. Obtaining funding from government sources requires continuous grant applications and constant claims of "innovation." This need to always find a new, outstanding output to sustain the platform disincentivizes maintenance or refinements to working systems. At best, measurement projects are forced to sustain their existing platforms and tools operations through contortion, sneaking in core components of the platform within new activities.[47] The constant struggle to secure enough funds to continue also creates hurdles where a limited set of large institutions that can manage uncertainty and bureaucracy dominate, but startup projects are effectively locked out.

Monoculture also forces many censorship measurement projects to associate themselves with a foreign government entity in order to fund their work. Whereas U.S. government funding is fine for American academic institutions, for a shutdown measurement program in Pakistan or Sudan, it could threaten livelihoods if discovered. Cultivating new funds from private sources would allow much needed alternatives that could open new

opportunities for collaboration and reduce the risks posed to participating organizations. These would allow projects in closed countries that cannot seek government funds to be able to conduct censorship measurement with less additional risk, bringing censorship measurement closer to the ground and making it more accessible to human rights defenders.

In the ECSA report, the authors noted several types of interactions that new funders would be better prepared to address than current sources:[48]

- Support interdisciplinary research, fellowships, and conferences to establish the scientific and methodological foundations of the space and enable evidence-pbacked policy-making;
- Initiate international academic partnerships and more collaborations with local organizations and international NGOs; and,
- Support stakeholders working in countries and regions where human rights online are at risk, and develop the capacity of local organizations to take part in the monitoring, analysis, and mitigation of incidents.

By acting independently, individual grantors can also use the power of the purse to promote better values within the community. For example, a series of workshops in 2014 on ethics in censorship measurement was funded in partnership through Tides Foundation, Knight Foundation, and the Open Technology Fund.[49] Private funding could also be tied to promote more collaboration and accessibility within the censorship measurement community. By ensuring that funding requires proper documentation to be maintained and the publication of analysis tools, it will be easier for future researchers in other regions to reproduce and build on top of existing work.

Rapid Response Censorship Measurement Funds

Funders should set aside a subset of money to provide strategic **rapid response support** where data-driven research and analysis can positively impact swiftly unfolding events. Instances of network shutdowns and application blocking have increased and spread to new countries in unexpected ways.[50] Readily accessible, low-overhead, and small grant funds would provide much needed flexibility to respond to these changes. These funds would differ from larger solicitations that provide more sustainable program support, and instead narrowly focus on providing technical materials and supporting dedicated research toward specific censorship events or regions. This would also provide a way to differentiate private funds from the lengthy bureaucratic process required by some government agencies.

Rapid response technical support for advocacy and remediation measures (such as information on how to circumvent restrictions) is extremely time sensitive. Due to the significant computational requirements for collecting and processing data, and the time required to do sound analysis of existing datasets, most current projects do not produce analysis until days, sometimes weeks, after an event. The current delays push past the time period where that data can be useful. Timeliness of findings is critical for building the media exposure and urgency in transnational bodies. As one interviewee framed the situation:

> *"When there are censorship events, external technical data from credible sources allows policy-makers to make a public statement or engage bilaterally with a country with evidence available. These are short-term opportunities. Engaging weeks later reduces impact because it is off the radar."*
>
> —CENSORSHIP MEASUREMENT DONOR

The current funding landscape for censorship measurement does not have mechanisms for supporting real-time measurement and analysis of unanticipated events. Better research, and more effective advocacy, can be done if censorship measurement projects have confidence that they will be able to recoup their initial investments in in-country testing equipment and hours spent on research, analysis, and outreach to local civil society and journalists. The best means to address this need would be allocating funds specifically toward rapid response requests in a capacity that allows short turnaround decisions. This could occur in coordination with or through existing rapid response mechanisms like the Digital Defenders Partnership or the OTF Rapid Response grant program.

Encourage Measurement Platforms to Document Methods And Data, and to Maintain Tools for Combining and Analyzing Datasets

The censorship measurement community should produce **robust documentation and develop tools that make it easier for other analysts to collect, transform, combine, and analyze the various data sets used in research and analysis.**

The independent and uncoordinated development of measurement tools has resulted in data that is difficult to directly compare. Analysis that is tactically useful for advocates often requires that one project's initial measurement data be enriched using a variety of other data sources. The identification, collection, and transformation of these other data sources is a difficult and time-consuming process that makes rapid analysis all but impossible. The issue of comparability was primarily raised by computer scientists and measurement initiatives (see Appendix I). They spoke of two specific challenges: the lack of common data formats and the lack of clearly documented workflows that would allow for the existing data to be transformed.

The reasons that such a cross-platform data format would be desirable are self-evident: platforms should provide analysts with an easy way to collect and combine the data from other sources. This would also help address other "wishlist" items that were raised in the interviews, such as automated sharing and analysis, longitudinal studies, and crowd-sourced analysis. Despite these needs, we are not recommending the immediate creation of a standardized format for measurement data as it is too early to impose harmonization. It would also be a monumental taxonomical task to create a single data format that can meet the unique needs of censorship measurement projects as well as the analyst community.

Engaging in work to support comparability and external analysis of datasets would act as a force-multiplier for existing analysis projects. Through this combined effort, analysts would be able to more easily reproduce and build on analysis from other regions collected by other projects. Over time, the censorship measurement community would organically develop clearer requirements for a robust community-wide standardized censorship measurement data format. Along the way, it will also be more clear what common formats would be expected to support. We see this recommendation as a way to provide the greatest short- and medium-term gains with respect to the current resource constraints of the community.

Shared Resources for Supporting the Public Presentation of Censorship Measurement Work

Effective communication of complex data analysis is always challenging. Censorship measurement data combines internet measurements, network terminology, and many other technical concepts that make it less accessible to the general public. Additionally, the censorship measurement community lacks sufficient capacity to effectively present and explain their findings to the groups who want to use them, such as journalists, activists, and advocacy organizations. Those who seek to use

the outputs from existing censorship measurement projects often discover the data that is available is, for their purposes, inappropriately scoped and inaccessible. There is a need for actionable data and information that can be understood and accurately used by external actors.

Outputs that are useful for one community are not necessarily useful for others. Researchers, data scientists, and human rights advocates may want access to raw results that they can build upon in their own work. Most journalists, on the other hand, are not interested in data for the sake of data. They need concrete evidence from a credible source to support a narrative. Censorship measurement projects have two primary types of outputs that need to be made more accessible: the collected data and contextual information from the findings. **We recommend addressing these two needs by promoting the adoption of common design patterns and lexicons for presenting censorship measurement data.**

Common Design Patterns for Presenting Censorship Measurement Data

Design patterns are generalizable, reproducible, and proven solutions to common problems. We recommend the creation and community adoption of **design patterns for censorship measurement data**. Design patterns would leverage a human-centered design approach to presenting censorship measurement data in consistent ways for different audiences. Design patterns focus on the types of interfaces, data visualizations, and APIs that are best for the different types of data and target audiences. Data design patterns are most commonly found within the style guides of organizations that work with a specific type of complex data[51] or as field and/or audience specific guides.[52]

These patterns will aid censorship measurement projects by helping consumers correctly interpret the data. The design pattern development process helps by identifying common types of interpretations (or misinterpretations), patterns of interaction, data structures, and system architectures that can then be applied as common techniques for sharing data, communicating analysis and findings, designing APIs, or even designing new tools.

The current lack of clear guidance around how to best present censorship measurement data to different audiences has forced each individual researcher and project to address this on their own. They have either had to learn how to organize, visualize, and communicate data themselves or to seek out funding to hire a designer to address their individual challenges. Given the resource constraints of this community, ongoing duplication of these efforts can be reduced through coordinated interventions from external specialists. With support from the design community, the initial creation of a common set of design patterns could be accomplished relatively efficiently. Once this initial collaborative process is complete, the community maintenance and ongoing contribution to these patterns would have to be supported. Additionally, by involving external design experts, the censorship measurement community would have skillshare opportunities to connect with the design community more easily and learn from their knowledge.

Donors can encourage this behavior through grant requirements, seeking in-kind support from design professionals, or providing ongoing individual research fellowships for maintaining these resources. Private-sector interviewees noted this as an area where they saw that they could provide expertise without duplicating existing measurement projects and a basis to deepen their interactions with the research community. Another possible source for sustainability would be to seek out a design consultancy that would be willing to provide long-term maintenance and upkeep of this project as a philanthropic project or in a continuing access service model, e.g. SimplySecure for OTF grantees or MAYA Design's support for Knight Foundation grantees.[53]

Common Lexicons for "Specific" and "General" Purposes

Over time, the preferred terms used by censorship measurement projects and advocates have changed in response to engagements with different communities and to accommodate different concerns. OONI has offered that "they are increasingly seeing that they need to update the terms they use because their audiences are changing." In the past, OONI has used "censorship" or "filtering," but the measurement community had shifted to different terms – such as "network anomalies" – in an attempt to depoliticize the research. However, OONI has found that terms like "anomalies" that hedge on the underlying causes have been confusing to important non-technical audiences, such as journalists and lawyers. Similarly, the use of "internet shutdown" had been extended to everything from disconnections to blocking, leading to the advent of "internet blackouts" to address the narrow situation of the cut off access. In effect, across the diversity of stakeholders with different perspectives, **the language used to describe a core issue—the purposeful interference of internet access—is fractured and has imposed its own veil of confusion.**

> *"Is it blocked? How do you define a block? We've got fairly clear guidelines for how we define [but] in some sense it is arbitrary where you draw the line. If you're losing enough data ... then we call it a block. Social media shutdown [means] severe throttling."*
>
> —TURKEY BLOCKS

Language is important since it can imply an understanding of scope or intent. For example, censorship often implies "government censorship," whereas "anomaly" suggests an unverified situation. "Information controls" and "interference" are broader terms that could also include legal and technical issues. Similarly, "network shutdown" appears to be increasingly used for application-specific blocking in addition to "disconnection of all connectivity." In practice, many cases are "alleged censorship," with attribution unconfirmed, unless a blocked page makes clear the intent behind the restriction.

Terminology is important for defining the scope of tools. The technical distinction between application-specific blocking for censorship and application-specific discrimination for economic purposes is non-existent. These nuances matter more in the policy and advocacy spaces where the question then becomes: does "network neutrality" constitute an interference, anomaly, blocking, or censorship issue? Does Twitter denying access to particular tweets based on the location of user fall within the scope of what should be measured? How do measurement platforms differentiate attribution and how is that communicated in aggregate or on a dashboard?

Other fields have addressed these kinds of complex terminology challenges by developing language dictionaries for both specific and general purposes.[54] The "language for specific purposes" (LSP) dictionaries are used to help experts translate or produce texts.[55] "Language for general purposes" dictionaries (LGP) are used to help a non-expert user understand expert texts.[56] We recommend the creation and community maintenance of LSP and LGP dictionaries for the censorship measurement space.

An LSP dictionary would be available for measurement projects when they are translating their results into actionable information for end-users. It would include:

1. Advice on words and phrases to use when describing specific types of censorship;

2. Plain-language definitions of key terms and findings that are less likely to cause confusion or misunderstanding;

3. Explanations of especially salient data points to provide alongside specific findings, such as what is being blocked, the source of the

block, level of confidence, and the duration of blocking; and,

4. Guidance on how to construct information to make it valuable for different consumers (e.g. summaries of censorship events provided to news media should aim for concise descriptions of fact, "the ISPs [List of names] composing [percentage]% of the internet connectivity in [country name] had no connectivity between [date-time] and [date-time]").

A LGP dictionary would be a resource that could be used by the consumers of censorship measurement information. This would help journalists, activists, and advocacy organizations understand and correctly interpret the information they are being presented by censorship measurement projects, including:

1. Clarifications to address common misunderstanding about specific terms and findings;

2. Distinctions between easily confused usages; and,

3. Common mitigations for specific mechanisms of censorship with links to easy to understand, and widely translated, guidance on implementing those mitigations.

Communicating an outcome of censorship measurement analysis usually involves combining multiple sources, such that the audience needs to understand both the data and the interdependent systems and projects in order to fully understand the findings. Currently, each project does this for their dataset, and the data that they use as part of their analysis process, rather than having a common lexicon across the community. These multiple, independent translations of data increase the overall costs of communicating censorship measurement information and contribute to the inaccessibility of the field.

By creating and maintaining shared languages, censorship measurement projects will be able to dramatically reduce the effort required to translate their findings to non-expert actors. Civil society could access the stock language, which reduces the uncertainty and technical barriers to participate in advocacy, including specific information on the type of censorship that was detected.[57] The general purpose language dictionaries provide a Rosetta Stone that will reduce the confusion that currently plagues those who seek to use the outputs of many existing censorship measurement projects and allow them to accurately translate the information for their own audiences.

With the support of an independent communications firm to lead the participatory process of creating these lexicons, the task could be accomplished relatively cheaply and quickly. Once this initial process is complete, the community maintenance and ongoing contribution to these lexicons could be supported with processes that are quite similar to those that were recommended for the design patterns in the previous section. These could be encouraged by various donor interventions, maintained through the support of a philanthropically-inclined communications firm, or maintained by an organization or community coalition.

CONCLUSION

The ideal vision of a centralized real-time dashboard for documenting, measuring, analyzing, and sharing information on internet censorship and disconnections remains limited by existing realities. However, small interventions and strategic investments can bolster the relevance of the community and build toward more harmonization. As we have documented through our interviews, the censorship measurement community has yet to connect over basic common needs or adequately coordinate its ongoing research with external stakeholders. A more effective data-driven conversation on internet censorship will require a stronger foundation and more communication. The current diversity of tools and initiatives is a strength in the field and should be further fostered through the collaborative structures identified throughout the report. Thus, consolidation of tools or platforms is neither desirable nor likely. Drawing from the recommendations, there are several intermediate steps that the community can begin planning for now that will foster more long-term collaboration.

These steps include:

- Convene current and potential censorship measurement funders to strategize around opportunities for providing resources for long-term maintenance and real-time analysis to measurement projects through existing and new funding structures.
- Establish a funded working group or coalition to focus on:
    - Fostering the development of collaborative structures for data-sharing and coordination; and
    - Encouraging measurement platforms to document methods and data and maintain tools for combining and analyzing datasets.
- Establish an independent non-profit intermediary to establish and develop a private-sector network information clearinghouse.

More collaboration among implementers and researchers will require investments in not only technology, but also people and support. Proposals outlined in this report, such as the inclusion of private data sources, require trusted and dedicated intermediaries. Although there is interest in collaboration, there is also a healthy skepticism among members of the community, stemming from resource scarcity and privacy concerns. At the moment, there are a few potential intermediaries who could play the roles of gatekeeper and coalition managers within the community. Determining the candidates and criteria of potential hosts for these roles requires a better understanding of the sustainability of funding resources and

continued conversations about trust among potential participants. The next steps should focus on collaborative trust building and increasing resources available to the community, which will in turn facilitate recommendations for data-sharing, resource-sharing, standardization, and deeper collaboration across the community and with the private-sector. These initiatives would provide the foundation for further cooperation toward community-maintained initiatives such as a dashboard on disruption and data-driven accountability on infringements of fundamental human rights.

APPENDICES

I. Scope, Limitations and Challenges of Internet Censorship Measurement

The interviews conducted with stakeholders were designed to identify the needs of diverse communities, particularly those requirements that were unaddressed. A full accounting of the barriers and dilemmas posed within censorship measurement is out of scope for this paper, as each different community faces its own challenges. Such an accounting of different profiles of stakeholders and their specific need would be a useful future exercise, and would be pertinent to recommendations related to improving the accessibility of technical information. This Appendix is intended to preserve some of the discussions and themes that arose within interviews to clarify certain recommendations and help stimulate further research.

Comparability

As a result of independent development of tools with different design philosophies and without daily coordination, the data produced by different measurement platforms is difficult to directly compare without intimate knowledge of each of the tools and datasets.[58] The issue of comparability was raised mostly by technical researchers and focused on the lack of common data formats as a key hurdle to cross-comparison. Outside of data representation, the differing measurement approaches lead to potentially divergent analyses. For example, if two tools provide different answers on whether a site is blocked, how would an analyst be able to account for or reconcile the difference? Is the difference the result of differing measurement vantage points, different methods, or other factors? Has the tool provided sufficient information to justify any interpreted conclusion, and can that be compared to the evidence of another tool? These are all critical questions that must be considered and, ultimately, answered.[59]

Test Coverage

Application or site-focused blocking and throttling: One of the primary targets of interference is

communications applications, such as mobile chat apps or social media. Measuring accessibility of specific applications is more difficult because unlike web sites or overall internet connectivity, they often implement custom protocols and obscure the implementation details of their service through proprietary code. In order to monitor even the basic availability of an application, the measurement tool would need to know in advance the IP addresses and domain names used in the application. While these internal properties can often be found by researchers (as well as governments attempting to engage in censorship) through reverse engineering, these interactions could be considered terms of service violations and subject to action by service providers. Additional complexity is added when attempting to measure the usability of the application (against, for example, application-specific throttling) by emulating the protocols used by the application. All of these factors are also subject to changes without notice, requiring constant updating and monitoring, adding complexity to the ability to reliably measure access to certain services.[60] As a result, in order to be thorough and accurate, a tool needs to be able to measure the full range of possible mechanisms of blocking but also targeted discriminations that degrade performance to deter use but do not completely block access.

Regional shutdowns and throttling: As discussed elsewhere, disruptions targeting specific regions or types of access are nearly as common as national disconnections.[61] While shutdowns limit the types of data that can be collected, there are datasets that can be informative. However, these datasets are often not well described or structured at the regional level, limiting their ability to describe scale or impact. Disruptions also do not have to be whole-scale disconnections from the internet. For example, rather than disconnect, some countries have historically throttled internet access during politically contentious occasions. From a platform perspective, throttling may appear like a sharp decline in users or usage, but not an overall drop off or a disconnection within routing data. Censorship is achieved just as well through these mechanisms, and when applied to limited periods, such as during a protest day, evening, or a security operation, it can become impossible to make strong assertions from limited and disparate datasets. Moreover, without context, these censorship events are difficult to distinguish from technical failures, such as a cable cut, interconnection dispute, or unrelated network issue.

Collection and Reporting

Measurement platforms also face a straightforward yet complex problem: how to detect a network shutdown if the reporting mechanism relies on access to the internet. RIPE Atlas has used the responsiveness of probes as an indicator of network shutdowns. The platform has thousands of nodes, often with hundreds or dozens in a particular country, providing a redundant and diverse perspective.[62] However, when one perspective represents the accessibility of a region, network operator, or country, it can be difficult to differentiate a technical failure with the measurement node from an outage.

Moreover, there is more to disconnections than merely a lack of access. Part of the assumed strategy of "national networks," such as in Iran, is to provide the opportunity to disconnect from the global network while providing access to highly-controlled domestic services. There is some indication, for example, that when North Korea has disconnected from the internet for long periods of time, it has kept some level of connectivity to China.[63] Thoroughly documenting such complexity requires measurement from within the affected area and cannot be produced from external observation. As a result, an ideal measurement platform should be able to detect shutdowns and perform subsequent data collection to document the circumstances and particularities of the incident.

The Human Factor Resources and Usability

Once data is produced, it requires someone that is interested to analyze and contextualize the data in a form that is accessible to non-technical audiences. Someone needs to tell the stories about how censorship compares across the world, or over time. Several interviewees, primarily those conducting the measurements, stated that there are not enough experts to analyze data. Human rights organizations similarly echoed that they were primarily reliant on local NGOs and technical partners as "fact checkers" to interpret or validate results, especially when the platforms produced reports that they knew were incorrect.[64] Most probes seem to require intermediate to advanced technical skills for its installation or operation. There is little to no automation for many of the current censorship detection tasks, and as such, it is very analyst intensive work. This will likely continue to be the case, as advocates need to ensure that the shutdown they want to call attention to is not the result of a network error or a false positive. This type of analysis is time consuming and there is little stable funding for analysts to conduct this work.

Ethics, Privacy, and Security

Concerns about the user risk involved in measuring censorship was a common and widespread issue among interviewees, and especially among platforms that coordinated the collection of measurements from user-hosted probes. In order to support informed choices about the potential risk of participation in measurement regimes, users should be able to account for the applicable laws and potential repercussions. This is not limited to the laws in the country, but an understanding of the political climate including: how often journalists are arrested, how tolerant the government is towards internet freedom in general, and if the government has a history of targeting civil society. In many of those cases, the situation is ambiguous and highly prone to fast-paced changes – what could be tolerated during moments of regime stability could quickly become a liability at moments of contestation.

Reproducible science and research is enabled by the disclosure of raw datasets, and an affinity to the open source ethos is closely held within the open internet community. However, as noted, disclosure has its risks, as it could enable retaliation against participants. Many platforms do not provide public data as a consequence of this concern. Under an ideal system without consideration of user privacy or potential harms, all data including IP addresses and packet captures would be kept, whether or not the data is disclosed. Granularity is important to understand specific results and to check the analysis, especially when the result is not normal. However, this data can pose a risk to the participants. As a result, platforms have typically made designs to omit certain data from collection in the first place, or cleanse it before storage, such as replacing IP addresses with Autonomous System Numbers.

II. Use Cases

Censorship measurement tools serve a variety of purposes and are, in turn, used as a means to a variety of different ends. For example, private and commercial operations may use these tools to focus more directly on service monitoring. They not only need to know that their service is down, they have to rapidly intervene to provide access to their users. Policy advocates tracking the same incident require evidence that proves that the event was, or was not, connected to their advocacy concerns.

Accounting for the motivations supporting measurement is useful in order to understand what data needs to be provided to different stakeholders. In short, understanding the motivations and goals can allow tool developers and others to create value within a broader ecosystem. Motivations might include, but are not limited to:

- Economic: focus on financial and monetary levers that can be used to grow interest in and need for censorship measurement and anomaly detection data;

- Operational: encompass those that are integral to a particular business model;
- Academic and research: highlight the levers of interest to academic research; and,
- Civic: cover a variety of stakeholder groups and uses, including journalists, NGOs, civil society groups, and other advocates.

The many use cases for these tools share overlapping requirements for the outputs they create from measurement data:

- Accuracy: accurately describe the event that has occurred;
- Attribution: able to be used to attribute the event to its origin or root cause;
- Comparative: comparable across regions and time;
- Compelling: make an intended impact to the target audiences;
- Contextual: describe the event as it relates to its surrounding context;
- Evidentiary: provide proof of when, how, or why the event occurred;
- Innovation: the outputs new or reached in a new way; and,
- Speed: produced and distributed rapidly.

The following chart offers a snapshot of several use cases, example tools, and necessary tool capabilities.

Category & Characteristics	Requirements	Example(s)
CIVIC		
Advocacy, activism, & public policy: evidence building and awareness raising	• Rapid • Accuracy • Comparative • Contextual • Compelling • Evidentiary	Internet Libre SFLC.in Internet Shutdown Tracker Turkey Blocks #KeepItOn Internet Shutdown Tracking & Toolkit
Journalism	• Rapid • Accuracy • Contextual • Compelling	

Category & Characteristics	Requirements	Example(s)
ECONOMIC		
Protecting business access	• Attribution • Contextual	Online services combating censorship/disruption targeting their services or companies
Ensuring large-scale access	• Attribution • Contextual • Compelling • Comparative	Department of State, international telecommunications bodies/groups (e.g., ITU, ICANN), RIPE Atlas, M-Lab
Calculating economic impact	• Comparative • Evidentiary	Brookings Center for Technology Innovation Impact Research, #KeepItOn
ACADEMIC		
Research	• Innovation • Evidentiary	Princeton, Berkman Klein, Citizen Lab, University of Massachusetts (ICLab)
OPERATIONAL		
Protecting user access	• Rapid	Companies dealing with being blocked as a side-effect of an untargeted disruption
Ensuring large-scale access	• Rapid	Circumvention tools examining how to circumvent wider censorship; local or nearby ISPs or network operator groups looking to ensure access and reliability under varying conditions, etc.

III. Selected Profiles

Reflective of the range of tactics that can be used in interfering with access, there are a number of approaches for identifying certain technical impediments.

INTERFERENCE DETECTION/CENSORSHIP MEASUREMENT Traditional understanding of how censorship detection is conducted. Coordinating with individuals inside the country to run a software client or host a hardware device that performs measurement to understand the experience from the perspective of the user.	
Open Observatory of Network Interference (OONI) https://ooni.torproject.org/	An open source and open data platform for detecting censorship, surveillance, and traffic manipulation on the internet.
Encore http://encore.noise.gatech.edu/	A browser-based measurement approach that collects data in cooperation with websites. Participant sites include a Javascript resource that forces the visitor's browser to make requests for third-party websites to see if the connection was successful. While browser security settings limit the type of information that can be measured in this way, failures can provide an indication about potential interference.
ICLab https://iclab.org/	A censorship measurement platform developed out of the computer science research community based on peer review methods. ICLab has different options for deployment – hardware probes, network tunnels, and software clients. While ICLab does not provide the same level of data disclosure as OONI, it does publish results online. ICLab has also produced research based on deployment in countries where censorship occurs and in partnership with civil society organizations.
Access Check	An academic research tool intended to be useable by a broad user base so that it can collect a significant amount of data. The toolkit runs on servers elsewhere on the internet, and relies on users to decide to queue tests to run at some regular interval.
Others	Country-specific platforms, such as: TurkeyBlocks (Turkey, Methodology), GreatFire (China), HikingGFW (China).

INDIRECT INTERFERENCE DETECTION/CENSORSHIP MEASUREMENT [SIDE CHANNELS]	
Open Observatory of Network Interference (OONI) https://ooni.torproject.org/	An open source and open data platform for detecting censorship, surveillance, and traffic manipulation on the internet.
Spooky Scan (Augur) https://www.cs.princeton.edu/~rensafi/papers/Ensafi2014c.pdf **Satellite** https://www.usenix.org/node/196211	Alternative to direct measurement platforms that enlists public-infrastructure in order to collect indicators of abnormalities or interference. Does not require the direct participation of users, which is thought to reduce some of the burdens of potential user harm and remove hurdles associated with enlisting and managing in-country volunteers. The downside is that this process is generally limited to a small number of protocols, TCP reachability, or use of open services such as DNS or HTTP proxies.
INTERNET MEASUREMENT Datasets or measurement tools that characterize impediments or changes to network accessibility beyond specific questions of censorious interference.	
Akamai https://www.akamai.com/us/en/about/our-thinking/state-of-the-internet-report/	Akamai is a popular Content Delivery Network (CDN) that provides aggregate data about the state of the internet from their vantage point. The company itself has more detailed data than they release for public consumption, but has made an effort to share data publicly at a level that can inform conversations around shutdowns.
CAIDA IODA https://www.caida.org/projects/ioda/	The IODA platform is a dashboard of internet outages sourced from aggregated datasets from active measurements of connectivity and passively-collected information from routing data or unique sources.
Dyn http://dyn.com/blog/category/research/	Dyn provides aggregate data about the state of the internet from their vantage points. The company does its own research and summarization of its data, which it publishes on its research blog. Dyn has been open to supporting and collaborating with the policy researchers and advocacy campaigns.
Measurement Lab (M-Lab) http://measurementlab.net http://viz.measurementlab.net	Measurement Lab is a collaborative project run by New America's Open Technology Institute, Google Open Source Research, and Princeton's PlanetLab to produce the largest source of open data on the health of the internet. M-Lab has servers in over 100 locations around the world, and hosts a variety of internet experiments that focus on different aspects of internet measurement. The flagship test is Network Diagnostic Tool (NDT), which focuses on web100 internet metrics (e.g. upload speed, download speed, and latency). M-Lab also hosts experiments more focused on censorship measurement explicitly: Neubot and Glasnost, as well as another popular general measurement tool, Bismark.
RIPE Atlas https://atlas.ripe.net/	The RIPE Atlas project is a global, open, distributed internet measurement platform, consisting of thousands of measurement devices located across the world that measure internet connectivity in real time.
Other	Background and alternative data sources, data collected incidentally by third parties from sources such as BGP routing data (e.g., BGPmon), and general purpose network access tools (ZMap, traceroute, Nmap).

SERVICE PROVIDER DATA COLLECTION	
Google Transparency Report Cloudflare Traffic Graphs Psiphon Traffic Graphs Wikimedia Page View Logs Tor Metrics	Another existing passive indicator of abnormality is the rate of activity on internet services. These can be as simple as the number of users reaching a site or network from a particular location. This information is often accessible already, but isn't disclosed at the same level of granularity out of concern for business confidentiality and user privacy. While this information is not as precise as end-user measurements, significant drops in user counts or traffic from a location, especially uniformly across mobile and terrestrial traffic can suggest a government-ordered disruption.
SOCIAL MEDIA REPORTS/CROWDSOURCED DATA Non-technical indicators, often anecdotal reports from users, have been the most common signal of problems even if not the most trusted from an empirical standpoint. In discussions with service providers and measurement platforms, it was commonly reported that news reports or social media chatter about certain situations were the first sign of problems.	
Herdict https://www.herdict.org/	An attempt to formalize and manage crowd-sourced information on web blockages as they happen, including denial of service.
RespectMyNet https://respectmynet.eu/	Crowd-sourced platform to collect cases of network neutrality violations and blocking, focused on Europe and oriented toward encouraging policy-makers to adopt strong net neutrality rules. This tool is more narrowly scoped and perhaps more reliable, and encourages visitors to adopt open tools.

IV. Interview Questions

Questions for Everyone

- What terminology do you use in describing purposeful restrictions on access to the internet or content (e.g. "censorship," "information controls," "anomalies")? What influences how you think about this topic? Are there political or social factors that shape your language? What about other factors?
- Have you observed censorship online? How do you define censorship?
- Are you familiar with tools that measure or track online censorship? What about tools that measure or track network connectivity or network anomalies?
- Why have you used censorship measurement tools?
- How have you used censorship measurement tools?
- What motivated your interest in the nature of censorship?
- Do you seek out information on censorship or online anomalies?
- How do you find information about censorship or online anomalies? What sources beyond your own observation or technical measurements do you use?
- What data is most important to you about censorship?

- How does this data contribute to your personal or professional engagements?
- Who else should we talk to?

Companies

- What are the indicators that you use to understand the status of your service in countries around the world?
- How do you assess whether your service is down or blocked in a specific country or region?
    - What operational telemetry is commonly used to determine accessibility?
    - Do you know every country that your service is blocked in at this moment?
- If your service was blocked how would you find out?
    - How would you know whether this was intentional disruption rather than a technical failure?
    - Who would you contact if you believe there were disruptions?
    - How often is the first indication of a potential blockage public reporting?
- Does your company participate in any public or private information sharing programs? What are they?
- What are the ...
    - Proprietary considerations related to sharing data – is it open, is it confidential but sharable, is it completely off limits?
    - Organizational considerations to sharing data? (competition, legal, etc).
- Would your organization be open to having outside groups implement tools to measure your service's availability?
- What data is currently accessible for developers via public or authenticated APIs? Shareable metadata?
- Do you provide documentation, specifications, and/or guidance on how your service works that could be used by outside groups to create an accurate emulation of your service for testing?
    - If not, if you were an outside group, how would you go about trying to measure the availability of your application?
- What of this data could you contribute to a broader data effort?
- What data would they contribute?

Policy Audiences

- What are your actual needs? What are your priorities?
- Exactly what type of data do you need? How do or would you use this data?
- What are the opportunities for policy audiences to use censorship measurement data for the purpose of advocating for positive change, e.g. organizations, international bodies, form of advocacy, etc?

Tool Developers/Maintainers

- Why did you decide to develop this tool? How did you go about developing the tool?
- What is missing from your tool? What do you wish it could do but can't?
- If you were to develop this tool again from scratch, what would you do differently? What would you keep?
- [If tool is defunct/failed: Why?]
- What is missing from the space? What is your contribution to the field?
- What forms of measurement data do you collect? What does your tool measure?
- Where does your data come from? Do you collect it yourself? Is it crowd-sourced? Submitted by third-parties?
- Have you collaborated with other(s) (individuals, organizations, companies) to compile and synthesize this data?
- What approach do you take toward deploying the tool and collecting measurements from interesting locations?
- Is the dataset publicly available? What restrictions exist on access to data collected by the measurement platform?
- At what rate of volume is data collected?
- Is the tool maintained?
- Is anyone outside of your project actively using the data that you collect? Who are they? What are they using it for?
- What other tools exist and what tools are similar to your tool?

Data-Driven Advocacy Efforts

- What are the reasons for running the data collection effort:
    - what goals do you hope to accomplish;
    - who is your audience; and,
    - what is your theory of change?
- What is your process for identifying censorship?
- Do you use an existing data collection tool, or have a custom developed tool?
    - Is that tool open source, and if not, what prevents opening the source?
- Is the data collection published in full? If not, what constrains the sharing of data?
- How do you do measurement? If there are multiple measurement points, how many measurement points are maintained?
- What design decisions have guided the collection of placement of data collectors?
- What privacy or security concerns have influenced the placement and maintenance of probes?

- Do you collect measurements from mobile networks?
- What is the relationship between the organization and probe hosts (e.g. paid, volunteers, affiliates, independent members of the public)?
- How is the measurement effort sustained financially? Is this sufficient and if not, what would you do if you had more resources?

Media

- What data on online censorship would be useful in your work?
- What are your priorities around that data?
- How do you want to interact with this type of service?
- Do you have other needs from a service like this beyond the basic information?
- Do you want raw data?

Other Stakeholders

- What are your needs?
- Why are you motivated to understand censorship issues?
    - What interests you about this topic?
    - How is it relevant to your work?
- Have you had previous experience working with censorship data?
    - In what capacity?
    - For what purpose?
    - With what data?
- What data in particular about online censorship would be most useful in your work?
- What are the communities you work with that are at risk for being subject to censorship online?
    - Why are they at risk for being censored?
    - How do you determine that they are at risk for being censored?
- Do you have direct engagement with affected individuals or organizations residing/working in countries that engage in censorship?
    - Are they national/regional/international public interest organizations?
- What are the sensitivities that shape your use of data and/or your ability to advocate for an open internet, or other behaviors?
- Do they feel that participation or sponsorship of research related to censorship endangers their ability to operate or could pose harm to staff?
    - Why or why not?

Notes

1 New America's editors follow the Associated Press style regarding the capitalization of internet. This is a contentious issue. Especially among internet researchers such as the censorship measurement community.

2 "Freedom On The Net Report". Freedom House. 2016. https://freedomhouse.org/report/freedom-net/freedom-net-2016.

3 "UAE: Prominent Academic Jailed For 10 Years Over Tweets In Outrageous Blow To Freedom Of Expression". Amnesty International. 2017. https://www.amnesty.org/en/latest/news/2017/03/uae-prominent-academic-jailed-for-10-years-over-tweets-in-outrageous-blow-to-freedom-of-expression/.

4 In 2015, there were at least 15 shutdowns of this kind reported. That number was dwarfed in 2016, when at least 56 shutdowns were reported. Access Now, as quoted in: Mikael-Debass, Milena. "More Governments Want To Kill Access To Twitter And Facebook. Here's How To Beat Them". Vice News. 2017. https://news.vice.com/story/more-governments-want-to-kill-access-to-twitter-and-facebook-heres-how-to-beat-them; "Facebook". Government Requests Report. 2017. https://govtrequests.facebook.com/; Larson, Selena. "Why Facebook Tracks Internet Outages Around The World". CNN Money. 2017. http://money.cnn.com/2017/03/12/technology/facebook-internet-blocks-kill-switch/.

5 Internet freedom is generally the principle that universal human rights are fully applicable to the internet.

6 Clinton, Hillary. "Clinton's Speech On Internet Freedom, January 2010". Council On Foreign Relations. 2010. https://web.archive.org/web/20161111152731/http://www.cfr.org:80/internet-policy/clintons-speech-internet-freedom-january-2010/p21253.

7 "Making sense of internet censorship: a new frontier for internet measurement." pg.84-89. ACM SIGCOMM Computer Communication Review 43.3. 2013

8 Fittarelli, Alberto. 2017. "Forecasting An Internet Shutdown: An Exercise With Indicators". Bellingcat. https://www.bellingcat.com/resources/case-studies/2017/04/19/forecasting-internet-shutdown-exercise-indicators/.

9 "Internet Shutdowns Cost Countries $2.4 Billion Last Year." The Brookings Institution. 2016. https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf.

10 Barry, Jaime Yaya, and Dionne Searcey. "Gambia's President, in Power 22 Years, Loses Election." The New York Times, 2016. https://www.nytimes.com/2016/12/02/world/africa/gambia-election.html.

11 Graham-Cumming, John. "Unrest In Gabon Leads To Internet Shutdown (Updated)". Cloudflare Blog. 2016. https://blog.cloudflare.com/unrest-in-gabon-leads-to-internet-shutdown/.; Kentanito, Ephraim. 2016. "Internet Shutdown In Zimbabwe: What Happened?". Access Now. https://www.accessnow.org/internet-shutdown-zimbabwe-happened/.

12 Filastò, Arturo. "OONI - The Gambia: Internet Shutdown During 2016 Presidential Election". Ooni. Torproject.Org. 2016. https://ooni.torproject.org/post/gambia-internet-shutdown/.

13 Nelson, Michael. "Will Autocrats Ever Learn? - The Internet Blackout In Gambia". Cloudflare Blog. 2016. https://blog.cloudflare.com/will-autocrats-ever-learn-the-internet-blackout-in-gambia/.; "The Gambia Requests For Data". Facebook. 2016. https://govtrequests.facebook.com/country/The%20Gambia/2016-H2/.; "Users". Tor Metrics. 2017. https://metrics.torproject.org/userstats-relay-country.html?start=2016-11-14&end=2016-12-14&country=gm&events=off.

14 Ultimately, diplomatic pressure and the threat of intervention from the Economic Community of West African States led to Jammeh leaving power. "Gambia Crisis: Jammeh Misses Second Deadline To Step Down". BBC News. 2017. http://www.bbc.com/

news/world-africa-38686144?ocid=socialflow_twitter.

15 Maclean, Ruth, and Emma Graham-Harrison. "The Gambia Bans International Calls And Internet As Voters Go To Polls". World News. 2016. https://www.theguardian.com/world/2016/dec/01/the-gambia-bans-international-calls-and-internet-as-voters-go-to-polls.

16 Toner, Mark. "Daily Press Briefing - December 1, 2016". Department of State. 2016. https://web-beta.archive.org/web/20161202113301/https://www.state.gov/r/pa/prs/dpb/2016/12/264717.htm.

17 Ileleji, Poncelet. "The Internet Shutdown In Gambia: Our Story" Association For Progressive Communications. 2016. https://www.apc.org/en/blog/internet-shutdown-gambia-our-story.

18 Schaake, Marietje. "Blocking Of Internet Access By Authorities In Cameroon". Foreign Policy. 2017. https://marietjeschaake.eu/en/blocking-of-internet-access-by-authorities-in-cameroon.

19 The notable exception is the OpenNet Initiative, which was cross-disciplinary and reached beyond academia to publish more accessible information on censorship from early on.

20 For example, the National Science Foundation funded project ICLab, currently based out of University of Massachusetts, has collaborated with the civil society organization Citizen Lab and Small Media to deploy measurement probes in eastern Africa and elsewhere.

21 "Ranking Digital Rights - Ranking ICT Sector Companies On Respect For Free Expression And Privacy". Ranking Digital Rights. 2017. https://rankingdigitalrights.org/.

22 "About Freedom On The Net". Freedomhouse. Org. 2016. https://freedomhouse.org/report-types/freedom-net

23 Although in interviews, one company had noted an incident where cultural sensitives appeared to be used as a pretense to block the service, and had to seek help from the government. Moreover, stigmatization is not only a concern for companies, as even measurement providers expressed concern that being too attached to anti-censorship advocacy could inhibit their operations.

24 "European Capability for Situational Awareness". pg. 26. European Commission. 2015. https://bookshop.europa.eu/en/european-capability-for-situational-awareness-pbKK0215595/.

25 Jones, Ben, Roya Ensafi, Nick Feamster, Vern Paxson, and Nick Weaver. "Ethical Concerns for Censorship Measurement". ACM. 2015. New York, NY, USA. http://conferences.sigcomm.org/sigcomm/2015/pdf/papers/nsethics/p17.pdf.

26 Benson, K., A. Dainotti, k. claffy, A. Snoeren, and M. Kallitsis. "Leveraging Internet Background Radiation for Opportunistic Network Analysis". ACM. 2015. New York, NY, USA. http://conferences.sigcomm.org/sigcomm/2015/pdf/papers/nsethics/p17.pdf.

27 To date, we could not identify a case of an individual being prosecuted for participating in a censorship measurement platform, it is easy to understand circumstances where users could face repercussions for such participation.

28 As part of OONI's web UI and mobile apps, the project has implemented a quiz that users are required to answer correctly (demonstrating their understanding of potential risks) as a prerequisite to running ooniprobe. Other measures allow users to configure OONI to increase or decrease the amount of precautions in performing measurements, such as which URLs are tested or how/where the data is sent.

29 Anderson, Collin. "Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran". eprint arXiv:1306.4361. 2013. New York, NY, USA. https://arxiv.org/abs/1306.4361.; Marczak, Bill. "time for Some Internet Problems in Duraz": Bahraini Isps Impose Internet Curfew in Protest Village". Bahrain Watch. 2016. New York, NY, USA. https://bahrainwatch.org/blog/2016/08/03/bahrain-internet-curfew/.

30 Often information of connectivity of networks within regions is not well described or structured, so BGP or traceroutes may not be informative, and will not describe scale or impact of a shutdown. While controlled testing by partners can augment some of this issue, the remoteness of certain regions – such as rural regions or areas with separatist movements – can be difficult to coordinate with. Kindzeka, Moki.. "Anglophone Cameroon Marks 50 Days Without the Internet". DW. 2017 . New York, NY, USA. http://www.dw.com/en/anglophone-cameroon-marks-50-days-without-the-internet/a-37841760?maca=en-Twitter-sharing.; Ranson, Courtney. "Government and Opposition Media Square Off over Zhanaozen". Al-Farabi News. 2012. New York, NY, USA: http://carnegieendowment.org/2012/01/17/government-and-opposition-media-square-off-over-zhanaozen-pub-46566.

31 The possibility of misinterpretation of data and subsequent incorrect conclusion of the data's significance was a concern that was voiced by several interviewees. As one interviewee highlighted NGOs, lawyers, and policy actors "want to tell stories based on the 'data," but have trouble identifying the especially salient data points, such as what is being blocked and the source of the block. Another data provider experienced the dangers of misinterpretation first-hand as their real-time monitoring page had to be taken down after the misinterpretation of the data led to false positives being reported in the news.

32 FOCI '17 - 7th USENIX Workshop on Free and Open Communications on the Internet. 2017. Vancouver, BC. https://www.usenix.org/conference/foci17.

33 "Issues: Internet Freedom". HumanRights.Gov. 2017. https://www.humanrights.gov/dyn/issues/internet-freedom.html.

34 "Information Controls Fellowship". Open Technology Fund. 2017. https://www.opentech.fund/requests/icfp.

35 The recommendations made here align well with the ECSA feasibility study published two years ago, and build on new developments and shifts in the community. 2013. "SMART 2013/N004 — European Capability for Situational Awareness". European Commission - Call For Tenders: Digital Single Market. https://ec.europa.eu/digital-single-market/en/news/smart-2013n004-%E2%80%94-european-capability-situational-awareness.

36 "Citizen Lab Summer Institute on Monitoring Internet Openness and Rights". Citizen Lab. 2017. https://citizenlab.org/summerinstitute/.

37 "European Capability for Situational Awareness". pg. 11. European Commission. 2015. https://bookshop.europa.eu/en/european-capability-for-situational-awareness-pbKK0215595/.

38 There are numerous public and private initiatives, and while outside the scope of the paper, examples include ThreatExchange, Community Emergency Response Teams (CERT), Department of Homeland Security's (DHS) Cyber Information Sharing and Collaboration Program (CISCP), and the Federal Bureau of Investigation's (FBI) Infraguard.

39 Collaborative structures could be implemented using a variety of different models, including: targeted campaigns on certain issues (e.g. shutdowns or specific regions), strategic partnerships, multi-stakeholder coalitions, or membership associations. The form that such an initiative would take depends on the goals and boundaries of potential members and can formalize over time. For example, while censorship measurement projects may be less inclined to directly collaborate on software development, there are opportunities for data-sharing that could be mutually beneficial to targeted campaigns. Additionally, even if measurement providers do not collaborate among themselves, there are unaddressed opportunities to foster cross-sector strategic partnerships to validate reports and improve data collection.

40 ProMED-mail; HealthMap; CIVICUS Monitor; Canadian Interagency Security Advisory Forum; The International NGO Safety & Security Association (INSSA), Humanitarian Data Exchange

41 Xynou, Maria, and Arturo Filastò. "Examining

Internet Blackouts Through Public Data Sources". OONI Probe. 2017. https://ooni.torproject.org/post/examining-internet-blackouts/.

42 "The Lumen Database". Lumen. 2017. https://lumendatabase.org/.

43 "Countering Cyber Threats Through Technical Cooperation with the Department of Defense". Homeland Security. 2016. https://www.dhs.gov/sites/default/files/publications/ST%20-%20Countering%20Cyber%20Threats%20through%20Technical%20Cooperation%20with%20the%20Department%20of%20Defense.pdf.

44 "Research at Google". Google. 2017. https://research.google.com/research-outreach.html.; "AWS Programs for Research and Education". Amazon WebServices. 2017. https://aws.amazon.com/grants/.

45 The U.S. government being the largest single donor in this space.

46 Pearce, P., R. Ensafi, F. Li, N. Feamster, and V. Paxson. "Augur: Internet-wide Detection of Connectivity Disruptions". Oakland: 38th IEEE Symposium on Security and Privacy. 2017. https://www.semanticscholar.org/paper/Augur-Internet-Wide-Detection-of-Connectivity-Disr-Pearce-Ensafi/50c17775ff6ed8c03fdca897742463fa72e1cc93.

47 An example is the requirements in Internet freedom allocations by the U.S. government. "Consolidated Appropriations Act, 2017". 115th Congress, 2017. https://rules.house.gov/sites/republicans.rules.house.gov/files/115/OMNI/CPRT-115-HPRT-RU00-SAHR244-AMNT.pdf.

48 "European Capability for Situational Awareness". European Commission. 2015. https://bookshop.europa.eu/en/european-capability-for-situational-awareness-pbKK0215595/.

49 Bullen, Georgia, and Chris Ritzo. "Exploring Frameworks for Ethically Responsible and Scalable Network Interference Measurement". New America Foundation, 2015. https://www.newamerica.org/oti/blog/exploring-frameworks-for-ethically-responsible-and-scalable-network-interference-measurement/.

50 Iraq's unique proclivity to shut down networks during testing days spread across the region. While global efforts such as the #KeepItOn campaign are attempting to hold governments and intermediaries accountable for repressive actions, there remains a dearth of technical evidence to build a record for accountability and advocacy. In part this is because the timetable of funds and program planning differ in scale from the immediate needs of those on the ground. Gibbs, Samuel. "Iraq Shuts down the Internet to Stop Pupils Cheating in Exams". the Guardian, 2016. https://www.theguardian.com/technology/2016/may/18/iraq-shuts-down-internet-to-stop-pupils-cheating-in-exams.

51 "OCHA Graphics Style Book: Representing Data". UN OCHA, 2011. https://docs.unocha.org/sites/dms/documents/graphicsstylebook_for_public.pdf#page=12.2; Cesal, Amy. "The Sunlight Foundation's Data Visualization Style Guidelines". Sunlight Foundation, 2014. https://sunlightfoundation.com/2014/03/12/datavizguide/.; "Service Manual - Design". UK: Government Digital Service, 2017. https://www.gov.uk/service-manual/design.; "CFPB Design Manual". The Consumer Financial Protection Bureau, 2017. https://cfpb.github.io/design-manual/index.html.

52 Visualising Information for Advocacy. The Tactical Technology Collective, 2014. https://visualisingadvocacy.org/getbook.; "International Business Communication Standards (IBCS®)". IBCS Association, 2017. http://www.ibcs-a.org/.

53 Additionally, there are community focused ownership models that could be relevant.

54 An annotated list of selected publications on lexicography, LSP lexicography, monolingual and bilingual LSP dictionaries. Nielsen, Sandro. Aarhus University, 2017. http://www.sprog.asb.dk/SN/publikationer.htm.

55 "Suggestions to Authors of the Reports of the

United States Geological Survey". United States Geological Survey, 2017. https://www.nwrc.usgs.gov/lib/lib_sta.htm.

56 "DATNAV: How to Navigate Digital Data for Human Rights Research". The Engine Room, 2016. https://www.theengineroom.org/wp-content/uploads/2016/09/datnav.pdf.; "A-Z Your Pocket Guide to Understanding Financial Terms". Dublin: National Adult Literacy Agency, 2009. http://www.simplyput.ie/downloads/plain_english_guide_to_financial_terms.pdf.

57 Or even to build onto this framework, logical flows of measurements or common methods of circumvention based on the detected mechanism.

58 The censorship measurement community is well connected and frequently discusses overarching topics in the field, however, coordination around specific technical implementation details and outputs is much more rare, creating a continued burden – especially for third parties that may be interacting with multiple measurement tools without being a part of those conversations.

59 Even where differences of methods and observation points can be fully accounted for, even minor differences in instrumentation within common network requests can make a significant difference in end results. For example, the Chinese and Iranian filtering regimes have proven to be in certain respects fragile – failing to censor during periods where the amount of traffic is believed to be high or unable to assess requests that are slightly differently formatted from what a normal computer would generate. These different potential sources of error speak to how difficult and timely it can be to full account for divergence in outcomes, even where everything is open source and transparent.

60 "Ranking Digital Rights - Ranking ICT Sector Companies On Respect For Free Expression And Privacy". Ranking Digital Rights. 2017. https://rankingdigitalrights.org/.

61 Table 2, Brookings

62 Aben, Emile. "Visualising Network Outages with RIPE Atlas". RIPE NCC, 2015. https://labs.ripe.net/Members/emileaben/visualising-network-outages-with-ripe-atlas.

63 Aben, Emile. "The Internet in North Korea - Hanging by a Single Thread?". RIPE NCC, 2015. https://labs.ripe.net/Members/emileaben/the-internet-in-north-korea-hanging-by-a-single-thread.

64 An example was provided about OONI reporting that TMZ was blocked in the United States, a claim that required spending time to refute.