Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Anonymity Networks: New Platforms for Conflict and Contention

Mina Rady

Political Science Department
Massachusetts Institute of Technology

2013

This material is based on work supported by the U.S. Office of Naval Research, Grant No. N00014-09-1-0597. Any opinions, findings, conclusions or recommendations therein are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

Citation: Rady, M. (2013). *Anonymity networks: New platforms for conflict and contention* (ECIR Working Paper No. 2013-2). MIT Political Science Department.

Unique Resource Identifier: ECIR Working Paper No. 2013-2.
http://dx.doi.org/10.2139/ssrn.2241536

Publisher/Copyright Owner: © 2013 Massachusetts Institute of Technology.

Version: Author's final manuscript.

MIT
POLITICAL SCIENCE

Massachusetts Institute of Technology
Political Science Department

Working Paper No. 2013-5

Anonymity Networks: New Platforms for Conflict and Contention

Mina Rady, MIT

Electronic copy available at: http://ssrn.com/abstract=2241536

Anonymity Networks: New Platforms for Conflict and Contention

Mina Rady
Visiting Student, Department of Political Science
Massachusetts Institute of Technology
minarady@mit.edu

MIT-Harvard ECIR Project

Abstract

Abstract: *Access to information is critical during population uprisings against repressive regimes. As a venue for information and data exchange, cyberspace offers many powerful social platforms for exchange of information. But the infrastructure of the Internet allows government to block or censor such platforms. In turn, anonymity networks emerged as conventional mechanisms for Internet users to circumvent government censorship. In this paper we show that anonymity networks became "terrains" for government-population conflict as they enable citizens to overpower governments' conventional control mechanisms over cyber-information exchanges. We delineate escalations of this cyber-conflict by studying two notable cases: Egypt, a simple case, and Iran, a more complex case. We take Tor network as the anonymity network that is subject of investigation. We highlight the range of actions that each actor can take to retaliate via anonymity networks. We conclude that design specifications and protocols of anonymous communication determine the strategies of escalation. Finally, we lay out the foundation for monitoring and analyzing dynamics and control point analysis of anonymous networks.*

This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research

Electronic copy available at: http://ssrn.com/abstract=2241536

TABLE OF CONTENTS

Electronic copy available at: http://ssrn.com/abstract=2241536

I. INTRODUCTION[1]

The Internet and its communication protocols allow, in principle, geographical and organizational mapping of senders and receivers. It is thus fairly straightforward for a government or an Internet service providing entity to localize, filter or monitor data streams flowing from/to a specific web service or from/to a specific geographical region. Several governments have utilized this capacity to control, monitor or censor Internet traffic. This control is exercised either directly, through Web Service Providers or through Internet Service Providers (ISPs). This reality has motivated both supporters of free speech and computer security researchers to investigate how non-governmental actors (particularly individuals) maintain their cyber-based freedom of expression and access to information without being compromised -- regardless of the filtering mechanism. Governments, on the other hand, which are driven by various political or regulatory motivations, seek to monitor and filter data transmitted across the Internet.

This conjunction of conflicting interests has shaped the domain of application for Proxy Technology. This technology ensures anonymity of client and server computers by "masking" the Internet Protocol (IP) address of the computer on the network. In this paper, we consider the most popular application of this technology, The Onion Routing (Tor) network. We show that activities conducted via and within this network reflect a new domain of political conflict between governments and their own populations.

The paper is organized as follows:

Part 1 introduces anonymity networks and their logic and then focuses on the Tor network, its components and operational mechanism. Then, we present the Tor data that will be the bases for our empirical investigation and contextualize data sources we are using to examine their reliability. This last step is important since Tor network measurements are for technical purposes, not for use in social science or political inquiries. Parts 2 and 3 examine two cases Egypt and Iran, and note the different actions and reactions that were pursued across anonymity networks. In Part 4 we present some generalizations from the case studies, list the actions/reactions that can be pursued vie anonymity networks, and place the investigations within a broader political and technical context. Finally we highlight new lines of future research.

II. PROXY TECHNOLOGY

2.1 Defining proxy technology

The technology of proxy networks is designed to obscure the identity of a user by masking the IP address. Since any data packet sent across the Internet must contain the IP address of its destination as well as the IP address of its source (Figure 1). The source must be included in the transaction for several reasons, most notably to let the destination know where to send its response to that data transaction[2]. Thus, any ISP, web service provider or an individual with off-the-shelve network sniffing software can probe any accessible point of the network and catalog source/destination IPs and contents of data packets transmitted and interfere with the data traffic in various ways.

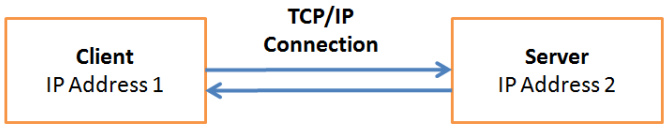


Figure 1 Typical HTTP connection reveals IP addresses of sides of the connection to each other

Several actors can intervene in network transactions. For example, (a) an ISP (either independently or influenced by a Government) can eliminate the communication if it is going to an IP address that is not permitted by the

[1] This work would have not been possible without the guidance and the intellectual support of Professor Nazli Choucri, MIT Political Science Department. Special gratitude goes to MIT ECIR research team as well as MIT COIN research group for their valuable input to this work.

[2] Another reason is to help assembling of fragments of each packet at the destination. Some packets are large in size and require fragmentation and then fragments may not travel the same route to the destination. In that case, the source of the IP address is necessary for the destination server to assemble fragments back into one packet.

Electronic copy available at: https://ssrn.com/abstract=2241536

jurisdiction of the ISP home country. (b) by mapping IP address prefixes to geographical regions, a web service provider can ban streaming of certain materials considered illegal in the recipient's jurisdiction, such as prevention of copyrights infringements[3].

Proxy technology offers a mechanism to evade those control mechanisms. The fundamental technique to circumvent such control is to deploy an "agent" (proxy) server as an intermediate between the source and the destination communication such that the IP address of the source (or the destination) embedded in the data packet is of the proxy server, not the actual source nor the actual destination. Therefore, any attempt to geo-locate the IP address of that source/destination will result into the geographical location of the proxy server instead (Figure 2).

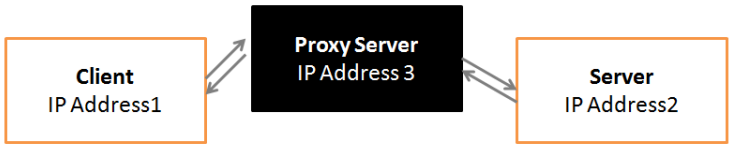


Figure 2 Intermediate Proxy Server is used to anonymize traffic from both sides of the connection

The traditional state system provides well-defined channels for both inter-states and intra-state attribution specially identifying illegal activities. Proxy networks challenge jurisdiction of states. Theoretically, the only way to overcome their challenge is by wholly re-inventing the Internet to "engrave" IPs of final source and destination into data packets transmitted (regardless of the rout they take) (1). Thus, it would be possible to determine the identity of the packet sender (2). Even with that re-invention, various attempts to define "identity" in cyberspace have demonstrated the ambiguity of identity. Therefore, the power of anonymity networks combined with the perplexity of cyber-identification, present unresolved challenge to enforcement accountability. (3)

2.2 Tor mechanism overview

Tor network is an amplified version of the basic single proxy server approach. Instead of providing one proxy server, Tor architecture provides a network of proxy computers -known as relays (Figure 3); such that, instead of data packets travelling across one intermediate agent, it travels across a *path* of proxy computers before it reaches its destination. This detour is the mechanism that ensures anonymity.

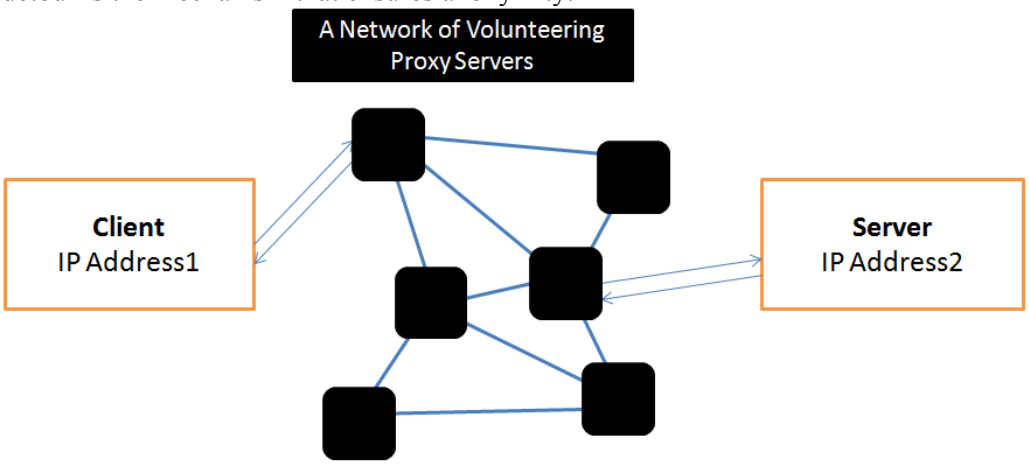


Figure 3 Tor provides a network of proxies instead of one proxy server

In order to realize this detour, while preserving the anonymity of the connecting users to the Tor network, the client computer selects a path of three proxy servers from the network (entry, middle and exit as in Figure 4). Then every data packet that is exchanged across Tor is encrypted multiple times (on the client machine) such that none of the participant proxy servers can identify the origin or the destination of the packet. Only the entry server knows the source and the exit sever knows the destination (4). Therefore, any partial observation of the network would not guarantee complete deanonymization of the traffic.

[3] For example, YouTube utilizes a Content ID system that identifies copyright infringements and bans the content from streaming to Countries that do not allow particular infringements (51).

Electronic copy available at: https://ssrn.com/abstract=2241536

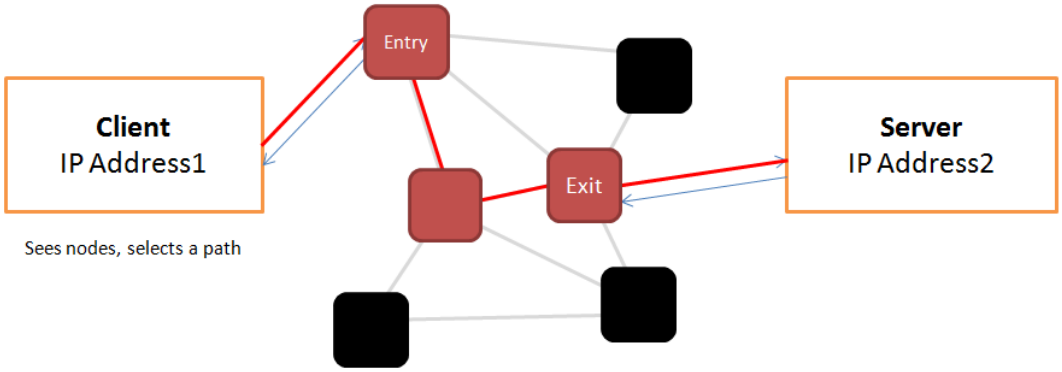


Figure 4 Data packets travel across three proxy servers for anonymity

We here highlight here different types of physical and logical components that constitute the Tor system:

a) **Relays**: computers that their owners volunteer to install Tor software on their operating systems and introduce them to the Tor network to be included among the proxies that perform the detouring of data packets. Any connecting user to the network will choose a random path that consists of a subset of the available relays to perform the communication; which stipulates that the IP addresses of these computers must be available to the public (5)

b) **Directory Authorities:** a subset of servers which are responsible for keeping track of a list of live relays and their operational statuses (in addition to other data). The list is updated on hourly basis and its purpose is to provide any connecting users with the IPs of the available relays. Then the client Tor software selects, randomly, the three nodes forming the communication path (6).

c) **Bridges:** subset of relays whose IP addresses are not publicized through the directory authorities' list; since the latter is public, it would be straightforward for any authoritative entity (Government, ISPs or web service providers) to block any Tor-based communication within their authoritative reach[4]. In contrast to relays, a user has to send an e-mail from a "Gmail" account to a Tor e-mail in order to receive only three IP addresses of bridges. Then a user configures the Tor client application to connect to one of these bridges. Therefore, filtering systems can only acquire the most minimal number of bridge IPs due to the inefficiency and restrictions of the "Gmail" acquisition mechanism. Thus, service continuity is ensured in case a typical filtering system is deployed by the ISP or the Government or any other entity (7). Figure 5 depicts this behavior.

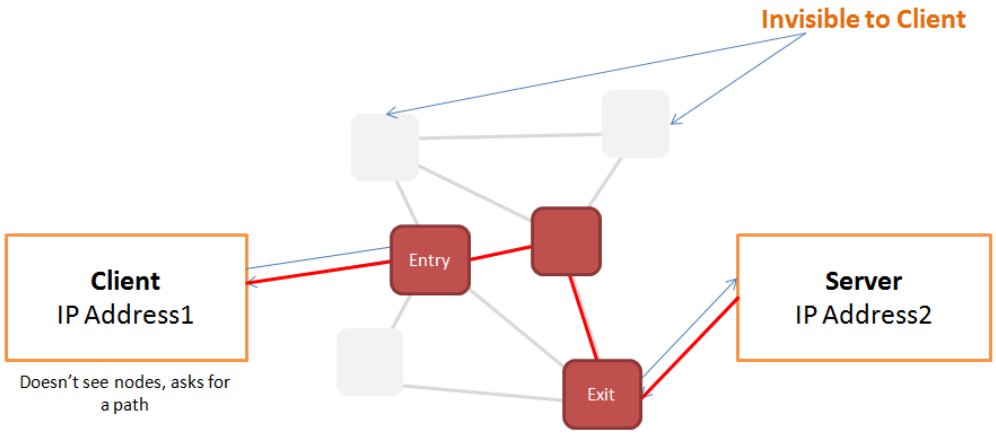


Figure 5 Tor Bridges: Only one entry point is known to the connecting client

A stylized visual abstraction of the network mechanism is shown in Figure 6. The figure is organized as following:

From left to right we note two successive phases:

- Phase I: retrieving the IP addresses of the three relay servers and

[4] Wikipedia is an explicit example of a web service provider blocking Tor. Wikipedia policy disables any access to editing Wikipedia content from a Tor relay. This is anchored to the abuse of Tor network by vandals. (52)

Electronic copy available at: https://ssrn.com/abstract=2241536

- Phase II: establishing the routed connection to the destination server.

Top and bottom sections represent two types of connections:

- Public relay mode: where IP addresses of all nodes are visible through directory authorities) and
- Hidden bridges mode: where only three IP addresses are revealed via an email response to a Gmail sender.

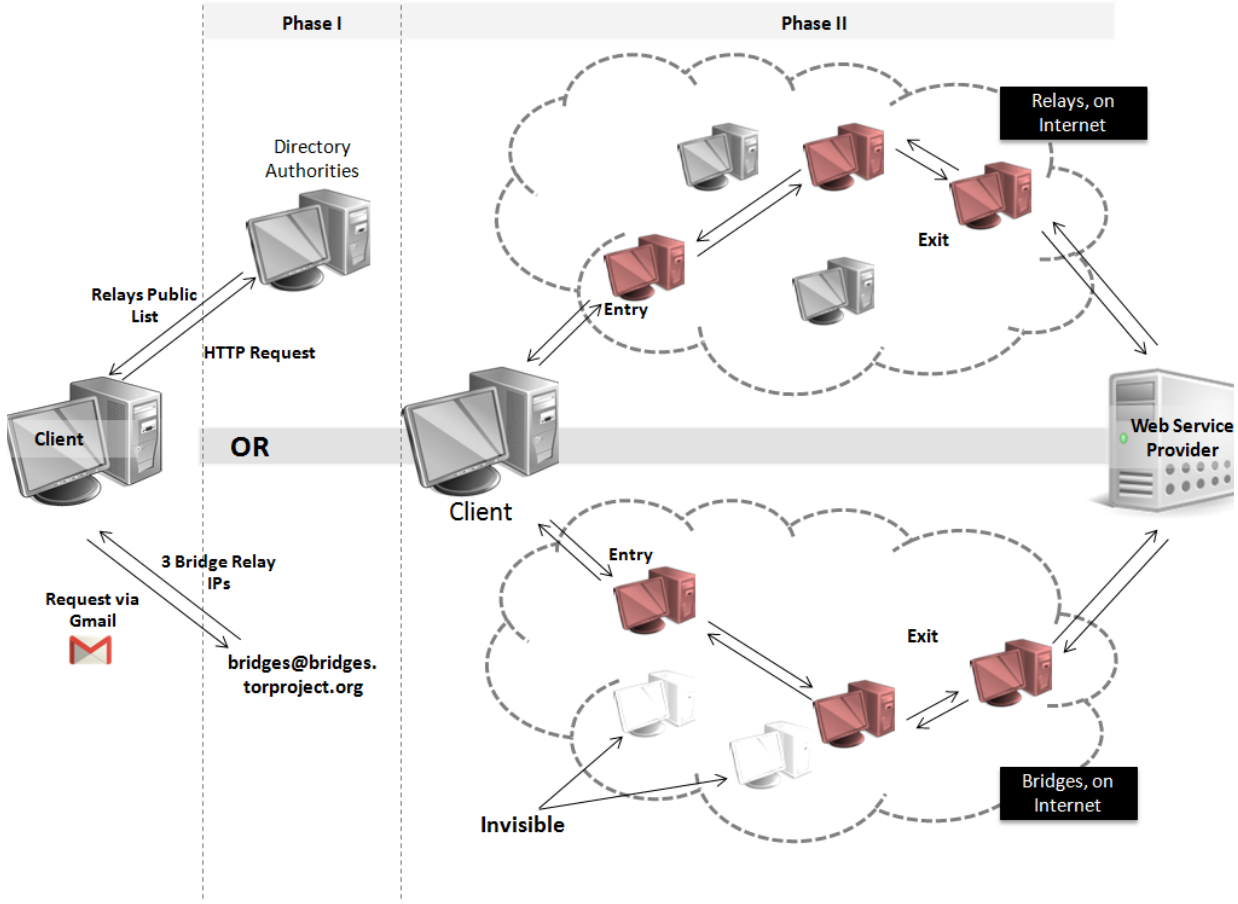


Figure 6 Overview of Tor Mechanism

The next section introduces the publically available Tor data, which we will use to examine our analysis of specific cases: Egypt and Iran as we contextualize them within their internal political dynamics.

2.3 The public Tor database

While the network preserves the anonymity of its users, at least in principle, the Tor project organization still disseminates data to the public that are "sanitized" of identity revealing information as well as general statistics about the performance of the network. Originally, the dissemination of this data was meant for technical purposes, such as: supporting the service by tracking its geographical accessibility and its performance; assisting computer networks researchers with assessment and optimization of the performance of the network under different circumstances; and providing different statistical data about relays to the public through directory authorities as explained earlier. The procedures to generate these measurements have been carefully designed to preserve the privacy and the anonymity of connecting users (8).

We describe a subset of the metrics provided by Tor project, which are the bases for our empirical investigations (9). Appendices I and II (available from the authors) contain a more comprehensive overview of available variables that we do not use in this paper, but might be of interest for other purposes. The metrics considered here include:

Electronic copy available at: https://ssrn.com/abstract=2241536

a) **Network Statuses log**: Data generated by directory authorities in hourly frequency to announce the list of all reachable operating relays that will be offered to any connecting client computer. It contains several attributes about each relay such as: IP address, Bandwidth and if it permits exiting to the Internet (i.e. allows being the last node in the detour that is exposed to the destination of a data packet).

b) **Server Descriptors log**: Self reported data by relays that constitute the Tor network since a server's details are considered by the algorithm that selects the proper path of severs to detour data packets (9). Those descriptors include, but are not limited to: Server Operating System, IP address, contact of the server operator and estimated bandwidth that the server can handle.

c) **Country Specific Data**: Aggregation of the above data sets with GeoIP open database. These aggregated data provides country specific statistics by mapping IP addresses provided by server descriptors and directory authorities report to GeoIP database and enables retrieval of existing records of IP addresses by country. We use this aggregation for our country-specific behavioral analysis. These metrics are provided across a timeframe since 2008 with daily frequency. Specifically, we use: numbers of directly connecting users (via relays) per country and numbers of connecting users (via bridges)[5] (9).

2.4 How to interpret the data

Here, we present the approach that would assist us to navigate and interpret the available data about access rates to public relays and that of hidden bridges.

We suggest that if the data show accessibility of public relays from a specific country (i.e. Tor is publicly available), then censorship is not highly practiced in that country. Since IP addresses of relays are exposed through the directory authorities (as explained in section 1.3), these relays are most prone to being blocked when a country maintains a strict level of censorship (8). However, spikes (positive or negative) in access rates to relays from a particular country are likely to signal the emergence of a censorship practice that may or may not be indicative of cyber politically-threatening activity.

We consider that an alarming signal of censorship activities appears if data show spikes (in the access to hidden bridges; Since IP addresses of bridges are only exposed through a very strict procedure that compromises the most minimal subset of bridges to connecting clients, bridges are highly likely to be used mostly in cases where public relays are either blocked or monitored. Although blockage of public relays is not common, government monitoring is possible and may reveal the content of packets transferred and potentially the entities involved in a Tor transaction and this might compromise their anonymity.

When we compare the public nature of relays versus the invisibility of bridges we suggest that that bridges are highly likely to be a default channel for high level security-related cyber-transactions (criminal, espionage or military etc.). Therefore, any unusual changes in the number of user access via bridges can indicate strong censorship practice[6] (10), especially if accompanied by a blocking of Tor relays (11).

To show how Tor metrics are relevant to politics, we take a foundational example for an association between Tor access rates and level of censorship per country.

We expect that the number of directly connecting users to the Tor network would relate to the number of Internet users per country. In figure 7 below we plot the number of Internet users versus number of directly connecting users to the Tor network per each country. We find, however, that some countries violate the expectation due to their censorship. For example, Tor has been fought very intensely in China. Therefore, even though China held the highest number of Internet users in the world in 2010 (around 460M users[7]), we observe that numbers of Tor users never exceed 4000.

Meanwhile, United States maintained an average of 33,000 connecting users to Tor throughout 2010 even though the total number of Internet users in 2010 was around 230M users. This figure is almost less than half of Internet users in

[5] Routing servers keep a geographically-mapped *count* of *unique* IP addresses that established a connection during a reporting period. The count's geographical distribution is reported with the Server Descriptors *at least* every 18 hours.
[6] In fact, this is the basic theory of an experimental censorship detection system created for Tor that is still being tested.
[7] According to World Bank Indicators Database

Electronic copy available at: https://ssrn.com/abstract=2241536

China. Similarly, Germany is marked for 22,000 users of Tor while maintaining about 67M Internet users, which is about 13% of Chinese Internet users. Unsurprisingly, China is categorized as enemy of the Internet by Reporters Without Borders (12) for its intense cyber-censorship policies, which are described in detail by the Open Net Initiative report on China (13).

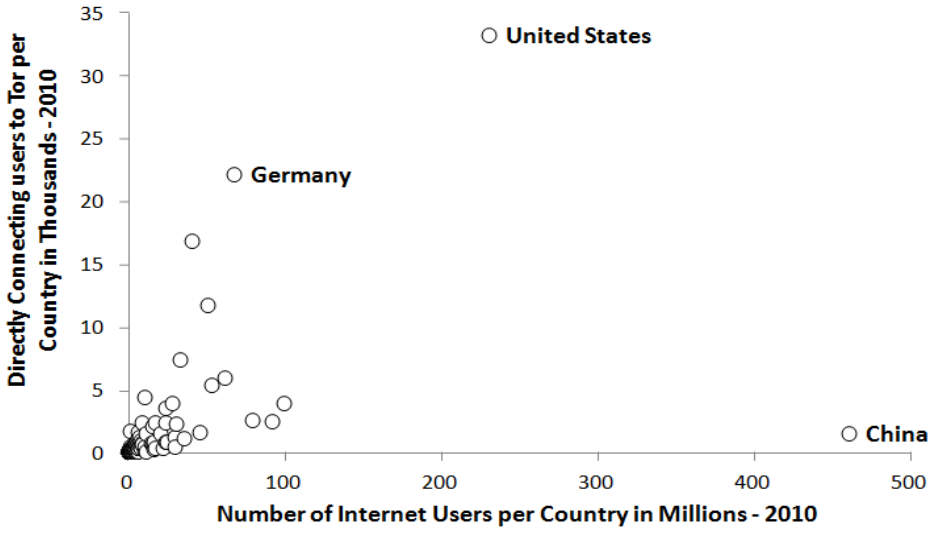


Figure 7 Number of Internet users per country vs. number of directly connecting users to Tor for each country in 2010

Figure 8 shows logarithmic scale of Figure 7 to illustrate the trend of cases at the extremes.

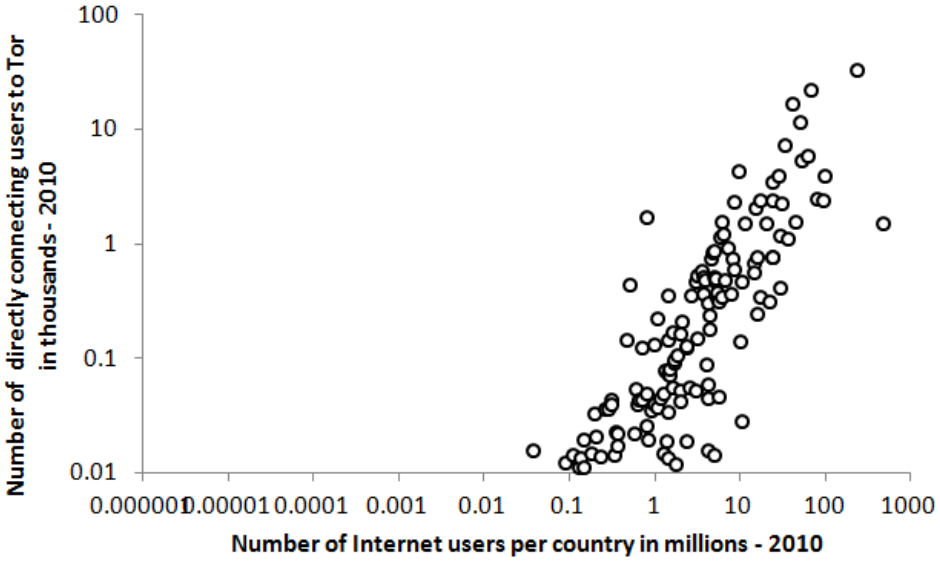


Figure 8 Previous figure plotted on base 10 logarithmic scale.

In general, the number of daily connecting users to Tor has increased across the past few years (Figure 9).

Electronic copy available at: https://ssrn.com/abstract=2241536

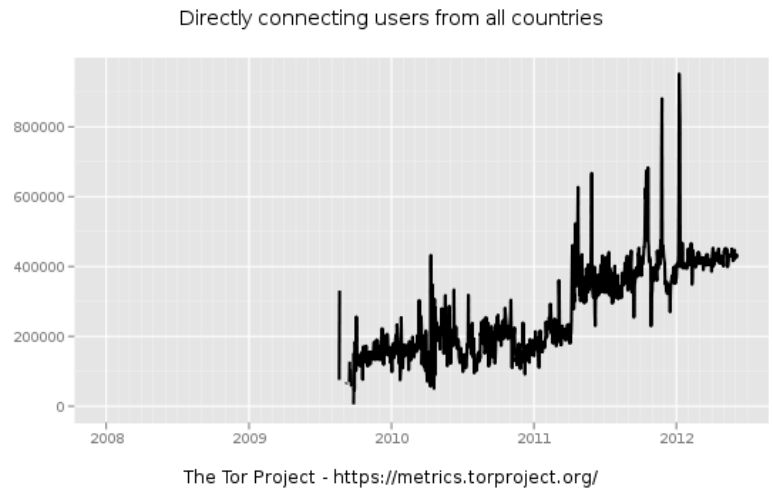


Figure 9 Aggregate directly connecting users

In the following sections, we examine (a) developments of states control of cyber-based information channels (b) intentions of their respective populations to leverage these channels for political discourse and (c) potential restructuring of intra-state conflict dynamics given cyber access. We expect that access rates of Tor from countries with repressive regimes to associate positively with perceived significance of cyber knowledge channels. Tor is a means for majority of Internet users to circumvent filtering. Therefore, we consider countries where it is clear that changes to proxy access rates are related to political contentions created by government censorship.

III. THE EGYPT CASE: ACTION/REACTION

3.1 The context

Since 2004, the growth of Internet users in Egypt has been dramatic. Figure 10, shows that internet users increased only to 3.5 million users during 2000-2004. But from 2004 to end of 2008, Internet users reached 16 million which is almost a 500% rise.

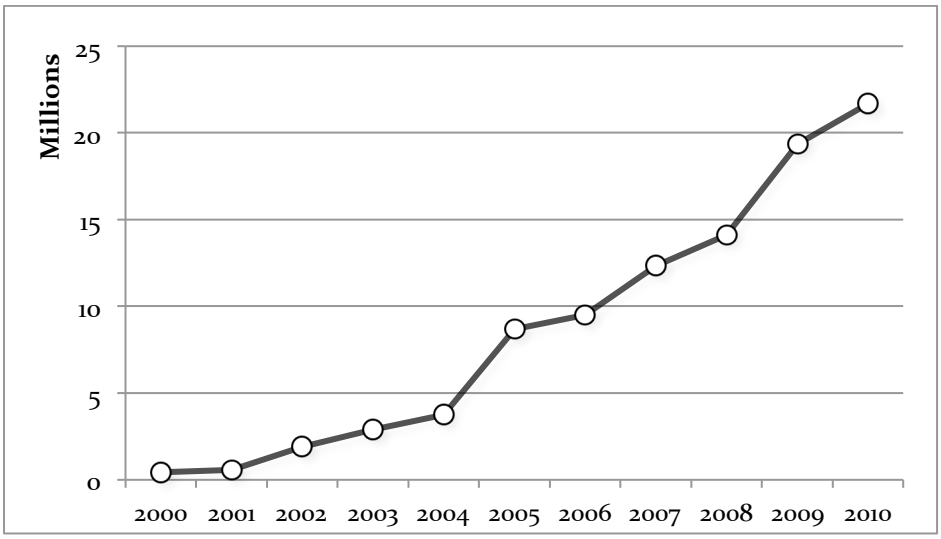


Figure 10 Number of Internet Users in Egypt

Created from: World Bank, World Development Indicators and Global Development Finance

In 2008, one of the earliest Egyptian nation-wide strikes took place on April 6. Workers' rights organizers planned a strike of 2700 employees to protest the low wages of a government-owned textile company (14). The strike

Electronic copy available at: https://ssrn.com/abstract=2241536

reinforced the public rage caused by rising food prices that began during the previous month (15). The call for a workers' strike motivated political activist groups to announce a nation-wide strike on April 6th (resonating with former Egyptian president Mubarak's 80th birthday). They publicized their call through their blogs and Facebook group and few local newspapers. On the same day the government responded by packing the capital with security forces (14) as well as in the locale of the original worker's strike north of Cairo. As many as 2000 protesters gathered in Tahrir Square, and at least 50 people were arrested (according to BBC news report). Later, the strike was reported to have failed in terms of achieving its demands for price reduction and for textile workers' regaining their rights (16). These events were the seed for the launch of 6th of April Movement, a politically active group, which sparked the beginning of intense political activism – and protests on the course of the following years. The launch began with a call for another strike on the following month, May 2008 (16).

Deployment of security forces in Cairo and the large number of arrests reveal the Egyptian government's latent caution early on to the impacts cyber-based information dissemination. It also signaled to youth activists the vitality of cyber access as a critical asset. This event also marks the first conflict in Egypt that spans both cyberspace and physical realm. Although the call for the strike echoed across the cyberspace, the government responded by deploying security forces across greater Cairo, Later, Egypt began the year 2011 with a huge bombing in Alexandria's Church of the Saints (January 1st). The news let to severe unrest in the streets of Cairo and Alexandria. Then the streets of Cairo witnessed the first reported "uncontrolled" clash between Egyptians and the Police forces which took place in the streets of Cairo, the BBC reports that during January 1st and January 2nd, Coptic Christians protested violently in several major streets in Cairo, attacking cars and protesting outside government buildings. The protests included heckling the ministers' cars when they came to visit the Coptic Cathedral and tear gas clashes with Police (17). Because those events were preceded with the overthrow of the Tunisian president, January 15th witnessed several demonstrations by political activist groups in Cairo calling for a replica of the Tunisian experience. The 6th of April Movement was one of the key organizers of these demonstrations (18).

Figure 11 summarizes the action/reaction chain described above in a form of process tracing. The two contenders in the conflict were: the Egyptian government and the Egyptian population (including Internet users).

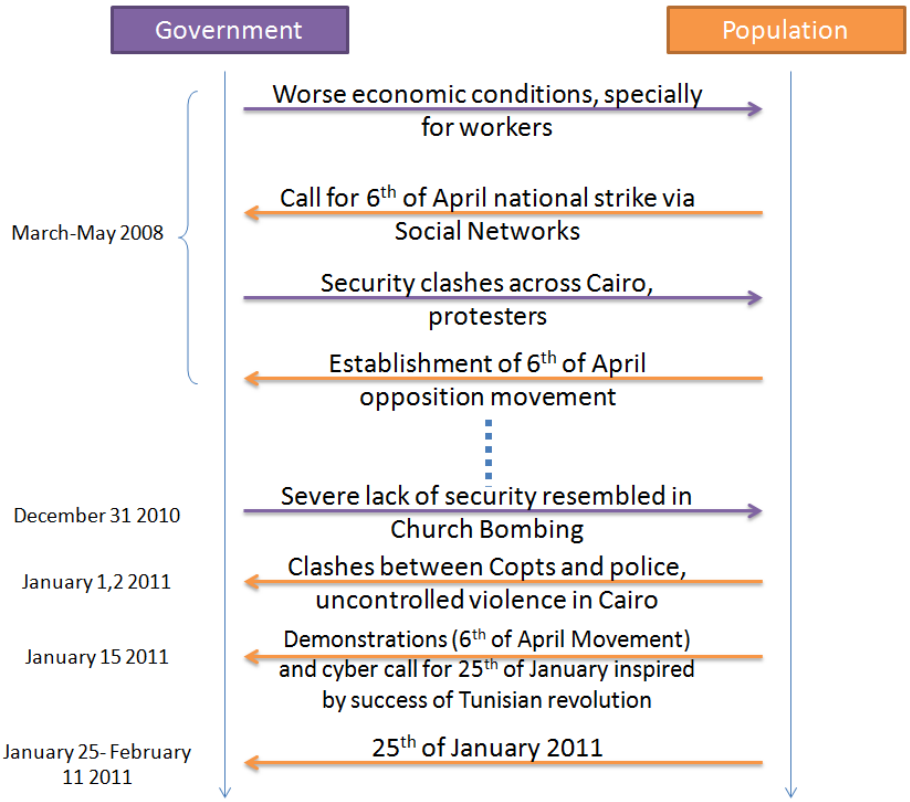


Figure 11 Action/reaction chain in Egypt before January 25th 2011

Electronic copy available at: https://ssrn.com/abstract=2241536

3.2 Government censorship: Cause/effect dynamics

To delineate the emergence of proxy technology (and Tor in particular), as a perceived point of power and leverage by both Egyptian Internet users and the Egyptian government during the January 2001 uprising, we note that:

1) The government perceived a threat in Egyptians' unprecedented interest in web-based information and social networking websites about plans for the protests, notably, locations of mass gatherings, call for supplies, reports of violence.

2) The government reacted to this perceived threat by blocking social networking websites (on January 26th)

3) Egyptian Internet users circumvented the governmental move by engaging in unprecedented high rates of access to proxy technology and

4) The government's final move, then, was to shut down the Internet (on January 28th).

The Conflict Dynamics:

Figure 12 summarizes the action/reaction chain of events. As in the Figure 11, we identify two main actors in the conflict: Government and the protesting Egyptian population.

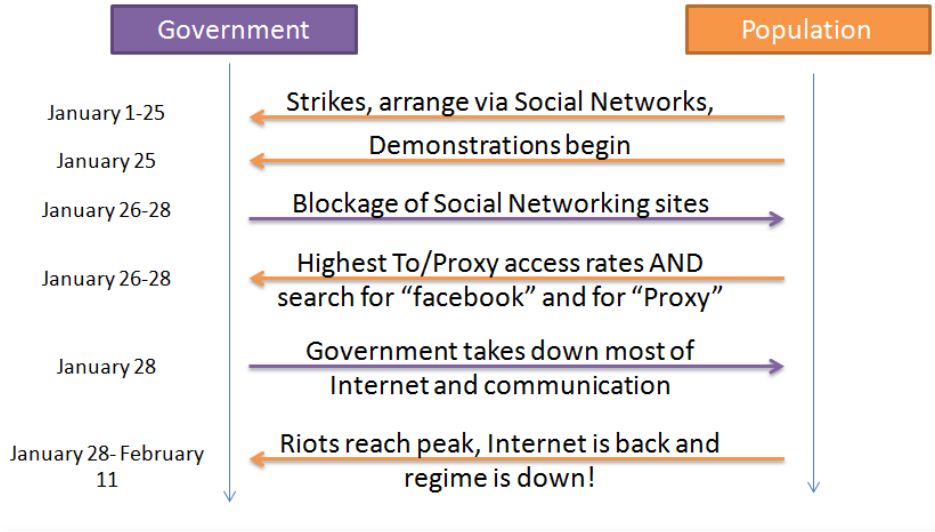


Figure 12 Action/reaction chain in Egypt during January 2011

In theory, the use of social networks as means to publicize and coordinate for 25th of January mass protests signaled to the Egyptian government the vitality of such cyber-medium to the continuity and survival of protests. With the severe clashes between protestors and Police forces on January 25th, it was apparent to the Government that continuous call for aid and mass calls on social networks as well as viral streams of clash footages were great strategic advantages to protestors. In fact, one can argue that social networking reversed the impact of the security forces in the streets of Cairo that it, instead of intimidating protestors, social networking motivated passive citizens to join the protests as they were informed of the great numbers on the streets as well as the violence against them. This unexpected positive feedback loop between social media and increasing numbers of protestors portrayed blockage of social networks as a reasonable action of retaliation from the government and for the obviation of further escalations. The moment social networks were blocked; however, proxy (anonymity) networks came into play as they were last resort for Egyptian Internet users to stay abreast of updates on the protests.

Electronic copy available at: https://ssrn.com/abstract=2241536

To empirically investigate how Egyptian Internet users' were strongly associated with proxy networks, we use the Google trends service. This service provides temporal-specific and spatial-specific, normalized[8], frequencies of search of specific key words. By querying the service, we obtained the search frequency history for the Arabic term for "the revolution"الثورة " - in red- appended to the search frequency for the word "proxy" -in blue- and we limited our query for search requests sent from Egypt based computers. Figure 13 shows these frequencies across the time-frame of nine years (2004-2012). The Y-axis represents Google's "Search Volume index" which a *relative* scale, its unit is the average search frequency for the queried terms over time (19) .

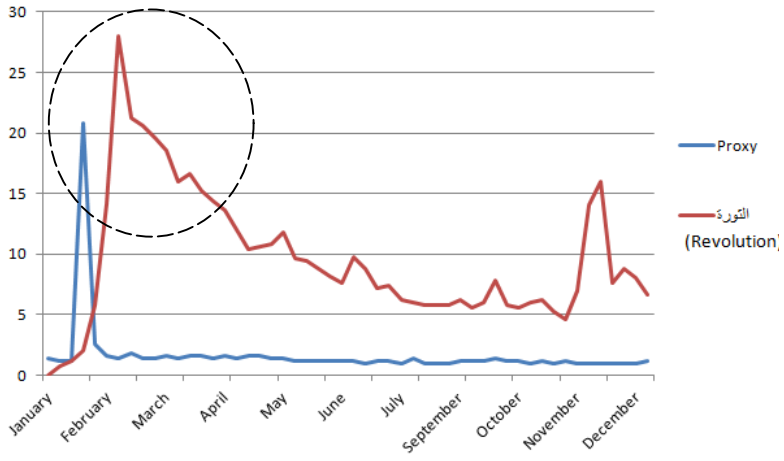


Figure 13 Egypt-specific Search trend for "revolution" or "الثورة" –red-and "proxy" –blue- (Span: Year 2011) [9]

Search trend for Proxy sites and networks in Egypt was congruent with search trend for the "revolution" during blockage of social networks. We can see that since early January, 2011, search frequencies for both the Arabic term "revolution" and the term "proxy" have reached a conspicuous peak. The search frequency for the Arabic term for "revolution" reached about 30 times average of 8 years[10], while the search frequency for "proxy" reached about 20 times the average of 8 years. More importantly, we observe that peak of search rates for "proxy" occurs right before Internet shutdown and reverts back to average after the Internet resumption. Demand to access Facebook specifically as mainstream social medium heightened during its blockage. We show Figure 14 the search rates for the term "facebook" from Cairo across the same time span. The spike resembles double the average frequency of search rates to Facebook which resonates with the time span of the Egyptians' uprise. This Figure shows that the peak between 26th and 28th of January. This is the time period when Facebook and other social websites were blocked and the entire shut down of Internet (where the graph is truncated due to unavailability of data)

Figure 14 Cairo-specific search rates for the terms "Facebook" (Span: January 2011)

[8] From Google trends information page: "All results from Google Trends are normalized, which means that we've divided the sets of data by a common variable to cancel out the variable's effect on the data and allow the underlying characteristics of the data sets to be compared. If we didn't normalize the results, and instead displayed the absolute rankings of cities, they wouldn't be all that interesting – a densely populated area like New York City would be the top city for many results simply because there are lots of searches from that area."

[9] Letter Labels that are appended to Google Trends Graphs are produced by Google, They are not of any meaning to this paper

[10] This data is relative based on the average of search frequency between 2004 to 2012. We had to include as wide time span as possible to ensure that these spikes in search are not frequent per year. (for example, Iran's search rates of the Persian word for revolution happen to rise dramatically early every year but during the celebrations of the Iranian Islamic Revolution)

Electronic copy available at: https://ssrn.com/abstract=2241536

Although we do not have the absolute count of search hits for both the Arabic word "revolution" and the word "proxy" from Egypt- since Google trends only gives away relative frequencies, we can imagine the magnitude of search hits about the "revolution" from Egypt. Comparatively, we know from the relative search trend for the word "proxy" (Figure13) that it reached about two thirds of the search hits for the word "revolution". It is definite as well that any search for the term "proxy" on Google returns hundreds of proxy services (such as Tor) that circumvent the Egyptian Government's censorship system. Therefore, we can confidently infer that accessibility to the Internet's blocked sites was *at least* two thirds the magnitude of search hits for the Arabic word "revolution", which is obviously is a huge number and thus huge accessibility, despite the circumvention. Similarly, Tor access rates from Egypt rise after January 26th. It is clear from Figure 15 that number of connecting users grew from about 500 to more than 2200 users. For sure, such high accessibility to proxies is counter to the Government's expected gain out of the blockage. Soon thereafter, complete Internet shutdown was the Government's last resort to evade further mass demonstrations. This move is also visible in Figure 15 as the number of connecting users dropped down to zero on the 28th of January. Thus, proxy networks were, in fact, a strategic cyber-leverage mechanism that, when accessed by the people, left the Egyptian government with the realization of the ineffectiveness of blockage and hence the escalation to a more economically severe and destructive cyber-action which is a complete shutdown of the Internet.

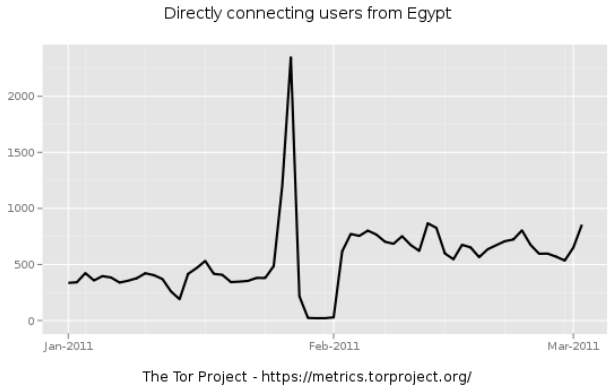


Figure 15 Egypt-specific statistics of directly connecting users to Tor network (Span: January-February 2011)

3.3 New regime: Ban on pornography

We now turn to different dynamics. In 2009, the Administrative Court ruled to ban pornographic web sites in a case initiated by an Islamist lawyer. The rule was celebrated by conservative Islamists as "Victory over Vice" (20). The rule, however, was not enforced. In February 2012, the post-revolution parliament, whose majority and president where from the Muslim Brotherhood's Freedom and Justice Party and Salafists' Nour Party, requested the enforcement of the ban (21). By March, the Supreme Court ruled to enforce the ban on pornographic web sites.

The response of the Egyptian "Cyber Population" (Internet Users) begins at the enforcement and is uncovered using Google Trends data. We find that the Supreme Court's rule accompanied a steep rise in search volume for the word "proxy" in Egypt. We see from Figure 16 that the search for "proxy" took place after the enforcement of the censorship by end of March 2012 [11].

[11] We can observe that search frequency for the word "proxy" goes back to average by beginning of June. This is probably because users would have marked down which proxy service they are using by June and began to access the service directly instead of "searching" for it.

Electronic copy available at: https://ssrn.com/abstract=2241536

Figure 16 Search volume for the term "proxy" from Egypt (January-August 2012)

The case of Egypt during January 2011 uncovers several questions related to power asymmetries in anonymity networks that may lead to future conflicts:

Can online anonymity continue to corner a government into shutting down of the Internet in case it is handicapped against uncontrollable traffic? Should any government have the "switch" to turn off the Internet, when and under what conditions? This question first proposed in the Christian Science Monitor (22). Not only is it a question of technical capacity but also a question of the availability of a policy option served by Governments' control mechanisms over ISPs combined with ISPs' control over the connectivity of their customers. And if "someone" can switch off the Internet, can this function be unilaterally initiated?

It is believed that not all networks were shutdown in Egypt on January 28th. Is such selectivity predetermined before the events of January and how was the decision made to take down specific network (as to: which networks and the means to take them down). Also, how can a governments escalation of filtering and control mechanisms undermine the performance of the national network and how much would it impact communication of critical network users (such as Military, Banks, Stock Exchanges, and Airports)

We highlight the case of Egypt with the following propositions:

1) Social media played a critical role in calling for and mobilizing for collective action (either via passive strikes in 2008 or via active protests in 2011). However, the impact of proxies and social networking in January 2011 was critical sparks leads to the subsequent events. With access to proxy channels, Egyptian Internet users prolonged their communication span, so that when Government decided to shut down the Internet the situation had already worsened well beyond tipping point.
2) This case is that of a repressive regime that can no longer enforce controls on the behavior of their citizens given their use of a communication technology initially based by a major power.

We are still left with a questioning about the Egyptian government's response to cyber-calls for strikes. The 2008 history shows that the Egyptian government was highly sensitive to the cyber call for a passive strike and, as a result, security forces were deployed in several parts of Cairo. By contrast, January 2011 began with much more strident alarms (Coptic clashes, Tunisian revolution and wide cyber call for a replica of the Tunisian experience). Unlike 2008, the Egyptian government did not seem to be sensitive or alert enough to gauge the scale of the revolt even with the alarming signals preceding it. This contrast is puzzling as it seems to uncover governance policy's incomprehension of aspects of the cyberspace that can always bear surprises.

IV. IRAN: CONFLICT AND COMPLEXITY

4.1 The context

In 2005, a survey of web blogs showed that Farsi (or Persian) ranked the third most common language of bloggers (23). Human Rights Watch report on Internet Freedom in the Middle East indicates that Iranian population has directed their attention to Internet based media -such as blogging- due to government's prosecution of independent media during the 2000s as more than one hundred independent newspapers and journals have been shut down since then. Meanwhile, Internet access in Iran boomed due to the activity of roughly 683 ISPs. (Iran has become largely

Electronic copy available at: https://ssrn.com/abstract=2241536

computer-literate and well connected) (23). See the World Bank trends in Figure 17.Internt use increased from about 610,000 users in year 2000 to about 5.5 Million users in 2005.

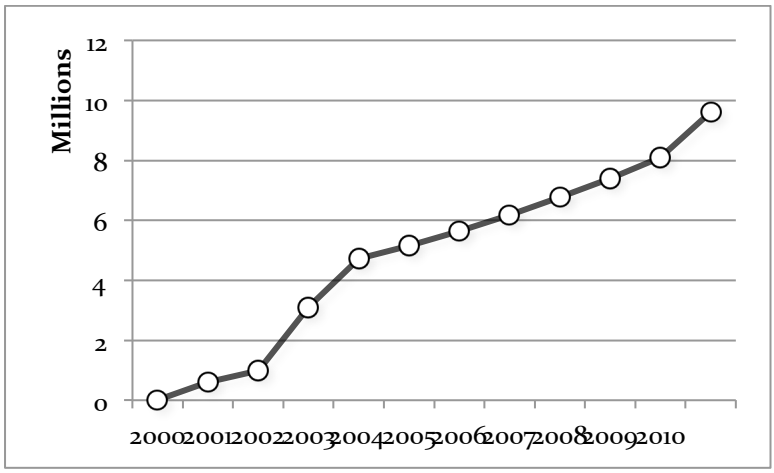


Figure 17 Number of Internet users in Iran

Created from: World Bank, World Development Indicators and Global Development Finance

We will illustrate how internal political instabilities contributed to a nation-wide increase in search for and access to the proxy technology and how this demand had impacts on this industry. We show that:

1) Iran's heightened access rates for proxy technology (other than Tor) since major arrests and trials of bloggers in 2004.
2) The 2009 presidential elections in Iran ignited political instability that heavily echoed across Youtube due to restrictions on the official media, which resulted into government's elevated restrictions on Youtube.
3) Since 2009 the growth in restrictions on Youtube, Iranians turned to Tor at rapidly increasing rates.

Figure 18 highlights the action/reaction dynamics that we shall discuss below.

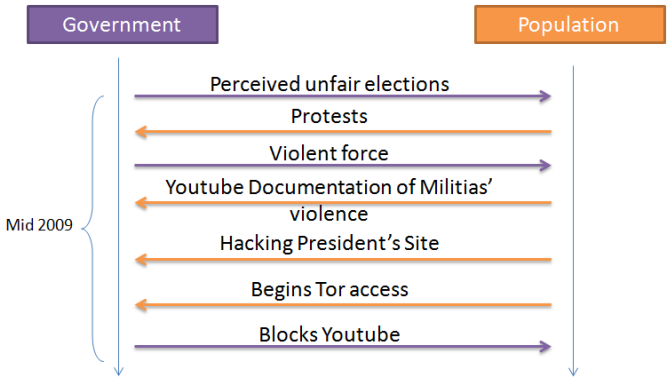


Figure 18 Illustrating Early action/reaction chain in Iran during 2009

Shortly thereafter, the Iranian government made three attempts to block Tor—on different occasions and with different reactions from the population and/or Tor engineers. The increasing sophistication of the blockage attempts has encouraged Tor engineers and users to deploy more enhancements to the operation of the system. These efforts resulted in overruling the government's own attempts. The overall effect of the government policy did not change access rates to the Tor service

4.2 Early demand for anonymity in Iran:

By 2004 Iranian government had already realized the potential threat of cyber-based freedom of speech. Between August and October 2004 about 20 bloggers and operators of online journals were detained because of content they

Electronic copy available at: https://ssrn.com/abstract=2241536

published that was deemed reformist or counter-government nature (23). In 2005, "Mojtaba Samiee"-a journalism student and blogger- was sentenced two years in jail for publishing blog posts that were considered "insulting" to the supreme leader Ayatollah Khomeini (24). This event was one of the earliest government reactions to cyber speech. Ever since then, dissident groups sites and blogs have been a targeted by the Iranian government as well as any sites that assisted in effort to evade government censorship (25).

In line with this heightened government's censorship, we find that Iranian Internet users generated the highest search frequencies worldwide for the word "proxy" on Google. By querying Google trends service, we find that when ranking world countries by search frequencies for the word "proxy", Iran heads the list for four consecutive years (2004-2007) and more specifically Tehran takes the lead in the list of world cities; also, among world language, the top language of search for "proxy" is Persian (Figure 19). Then Iran comes in second place after Kuwait in 2008, 2009 and 2010 for search frequencies for that term.

Regions	Cities	Languages
1. Iran	1. Tehran, Iran	1. Persian
2. Vietnam	2. Riyadh, Saudi Arabia	2. Vietnamese
3. Kuwait	3. Bucharest, Romania	3. Romanian
4. United Arab Emirates	4. Chennai, India	4. Russian
5. Indonesia	5. Bangkok, Thailand	5. Arabic
6. Saudi Arabia	6. New Delhi, India	6. Thai
7. Russia	7. Sao Paulo, Brazil	7. Portuguese
8. Romania	8. Taipei, Taiwan	8. Turkish
9. India	9. Sydney, Australia	9. Polish
10. Philippines	10. Milan, Italy	10. English

Figure 19 World rankings of search for the term "proxy" on Google trends in 2004 (By Country, City and Language)

Figure (20) shows the search requests from Iran throughout year 2005 for the term "proxy". Meanwhile, conviction of arrested bloggers by the Supreme Court peaked from March to May 2005 (23). Further, the peak in Figure 20 is in 2005 when the major trials of Iranian bloggers took place.

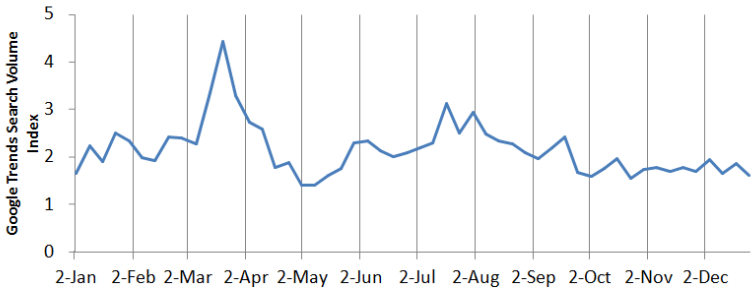


Figure 20 Search requests volume index for the word "proxy" in Iran in 2005[12]

4.3 Presidential elections voters/government reactions on YouTube:

Another wave of online censorship took place during and after the Iranian presidential elections in the second half of 2009. The Washington Times reported the massive protests that flooded the country after President Ahmadinejad was believed to be handed office after unfair elections. The BBC reported that the social media was the main channel that enabled mobilizing hundreds of thousands of protesters. Hackers were also reported to have taken down the website of Mr. Ahmadinejad as an act of "cyber disobedience" (26) (27). The protests resulted in severe and violent responses by the Iranian Militias, which appeared also as enormous raw video material of recordings of violence by the government's Militias (28). All videos were shared through YouTube, which led to heightened global media attention (28). As a result, the government placed higher restrictions on access to YouTube.

To show the heightened restrictions on YouTube, we use Google's Transparency Report, a service. That provides interactive visualizations of normalized access rates to specific Google services per country[13]. These include access

[12] Letter Labels on Google graphs are used on the original source of the graphs for a purpose that is not relevant to this paper.

Electronic copy available at: https://ssrn.com/abstract=2241536

rates to about 16 services, including YouTube. Figure 21 shows the sudden censorship imposed by the government on access to YouTube on June 13, 2009.

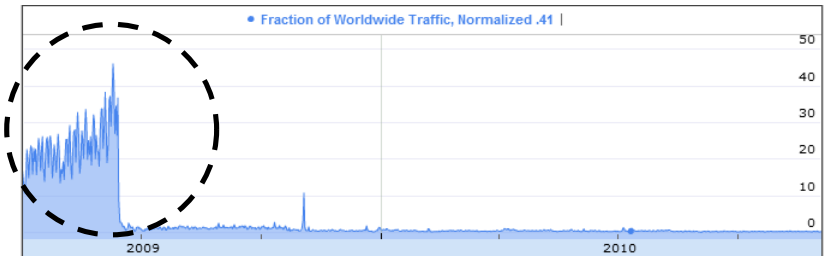


Figure 21 YouTube Iran Traffic Divided by Worldwide Traffic and Normalized (from Google Transparency Reports)

4.4 Early Iranians' activity on the Tor network

By looking at both rates of directly connecting users from Iran to Tor (Figure 22) versus numbers of users accessing via hidden bridges (Figure 23), we find that, Iranians' first interactions with Tor were through the hidden relays, beginning May 2009. Public relays were first used in September 2009 in the midst of the disputed presidential elections

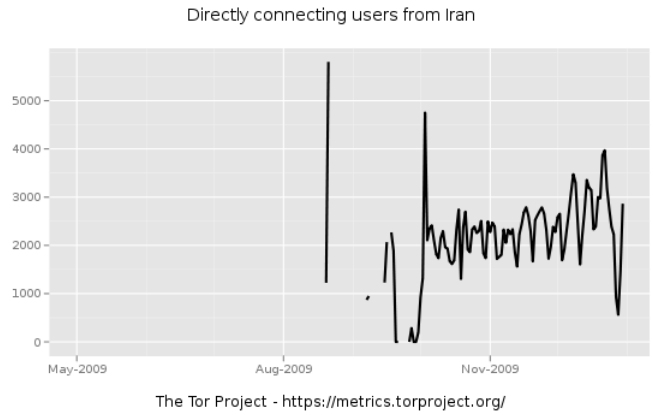


Figure 22 Directly Connecting users from Iran (May-November 2009)

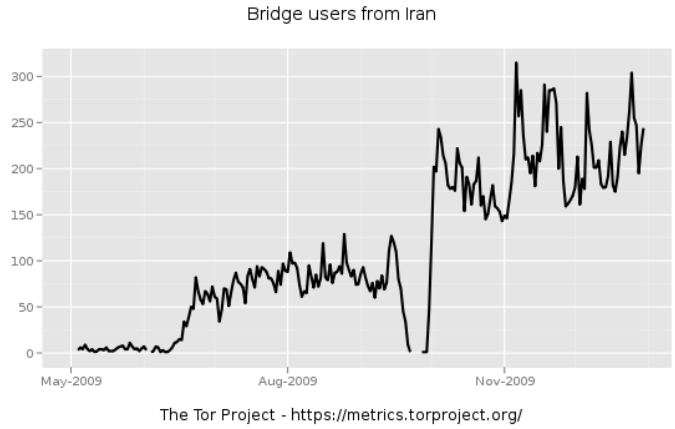


Figure 23 Bridge users from Iran (May-November 2009)

Since then Tor witnessed increasing rates of access from Iran, reaching 90,000 users early in 2012 (Figure 24).

[13] This report provides access rates to the following services: Gmail, Blogger, Google Books, Google Docs, Google Earth, Google Groups, Google Images, Google Maps, Google News, Google Search (Unencrypted), Google Sites, Google Spreadsheets, Google Translate, Google Videos, Orkut, Picasa and Youtube.

Electronic copy available at: https://ssrn.com/abstract=2241536

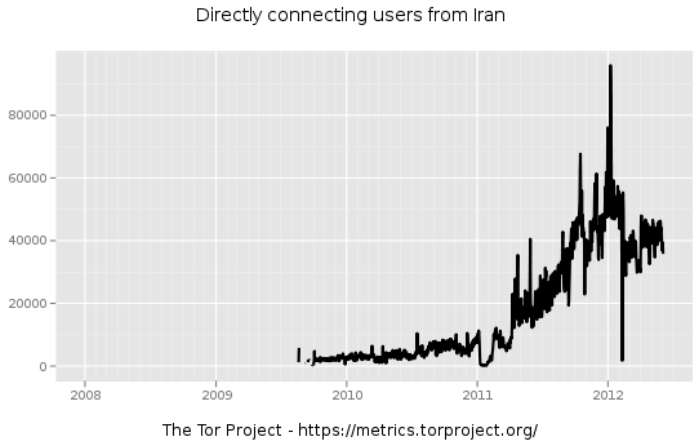


Figure 24 General Increase in Access rates to Tor from Iran

Unlike the case of Egypt, The conflict of interests between both the government and the Iranian population has generated technical evolutions of the Tor network infrastructure itself. To illustrate these dynamics, we turn to three episodes of escalating actions/reactions. The action usually begins with a government move, *first* to *distinguish* Tor traffic and *then* to block it. Supported by US based Tor engineering researchers Iranian Internet users react with support of Tor (29)- by adopting researchers' enhancements of the network to outrun the government's censorship model.

i) First episode, January 2011

The first reported attempt by the government to block Tor and other circumvention tools was in January 2011. The online archive Tor project reports (30) a complaint by Iranian Internet users for connectivity problems, however not just with Tor but also with other circumvention tools[14]. It later turns out, as reported by Tor engineers, in the attempt to trace the problem, the Iranian national firewall was updated to almost completely block any SSL-based (encrypted) communication over the network (30). Since the Tor public service requires by default SSL connection (to hide its content from public network sniffing), and since SSL connections are established by default via port 443 on a computer in the network, the blockage seemed to interrupt any communication to/from port 443 and hence the Tor services were affected. However, Tor engineers advised (30) Iran-based users to connect to bridges that are not using port 443 for SSL communication (since the national firewall, hypothetically, blocked communications to/from that particular port. As a consequence, Iranians access to the Tor network (either via relays as in Figure 25 or via bridges as in Figure 26) was suppressed during most of January until they adopted the change in port.

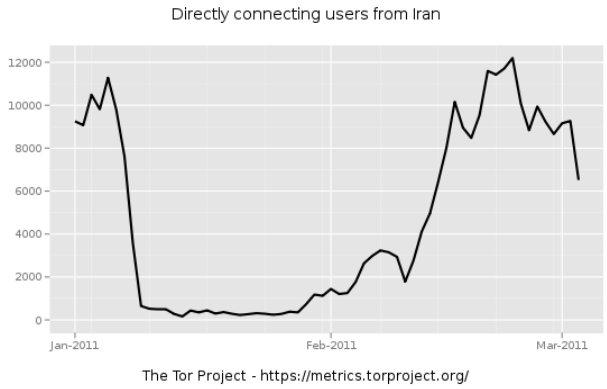


Figure 25 Access to Tor relays has been suppressed in Iran during January 2011

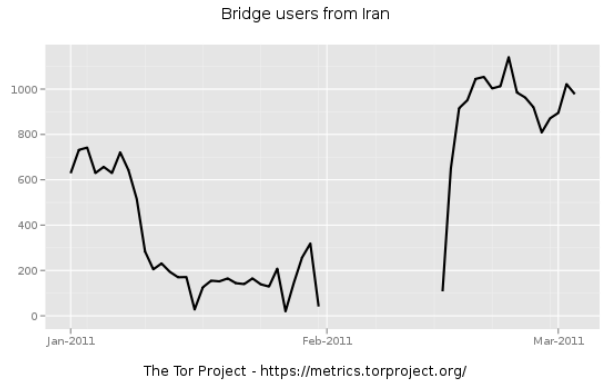


Figure 26 Access to Tor bridges has been suppressed in Iran during January 2011

[14] Such as UltraSurf, Freegate and Hot Spot Shield

Electronic copy available at: https://ssrn.com/abstract=2241536

ii) Second episode, September 2011

The second attempt by the government to block Tor took place during September 2011. It deployed a slightly more sophisticated approach to distinguish a Tor connection. Since Tor connections follow SSL protocols, it requires a secure certificate with a certain expiry period to be established between the nodes of the SSL based communication. The default expiry period of a certificate of any SSL-based connection is one year (31). However, Tor programmers had that certificate expire and renew every two hours, a very short time compared to the normal expiry period. Therefore the national censorship system of the government was, we assume, instructed to block any connections with very short expiry certificates, which worked effectively for few days. Later, Tor engineers updated the system such that the expiry period of the SSL certificates of the Tor connections falls more within the average normal period of a regular certificate (31). Figure 27 shows the impact of this filtering attempt on the number of directly connecting users from Iran (it went down to 20,000 and later up to 40,000 users):

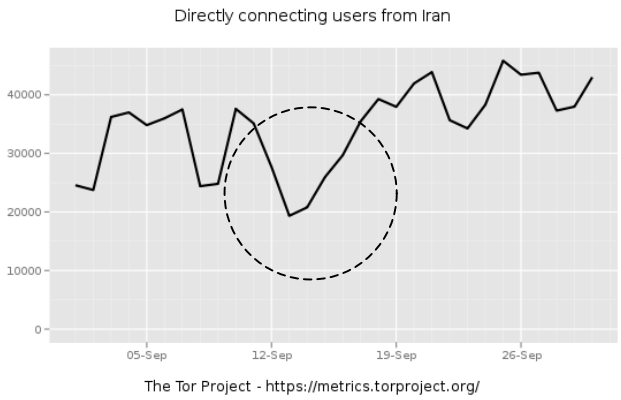


Figure 27 Impact of second blockage attempt

iii) Third episode, February 2012

The third attempt of Tor blockage, came during February 2012 before the parliamentary Iranian elections in March and in line with several activist groups call for protests against authoritarian rule. Computer Business Reviews reported that Iran had attempted to block SSL based communication based on more sophisticated approach that filters packets by their contents rather than their external attributes (32). This blockage attempt had impacts across global media because of its technique and timing.

Investigations of Tor engineers reported that the Iranian government was deploying Deep Packet Inspection (DPI) (33), that is, applying algorithm that inspects the contents of the transmitted package for any undesired content (regardless of the source and the destination). This algorithm for example, filtered out any search requests that contained the specific words such as “Tor” and any communication to the IP address of the Tor project website (33).

Figure 28 shows that the blockage had severe impacts on access to Tor from Iran (In addition, access to Gmail encrypted services was heavily disrupted. Figure 29 shows the sharp drop down in access to Gmail service from Iran. In reaction, Tor has announced that it was creating an “obfuscation proxy” module to counter DPI measure (34). The module is designed to change the look of the transmitted data packets so that the DPI algorithm would fail to recognize that packet contents are encrypted and hence would let it pass through the firewall.

Electronic copy available at: https://ssrn.com/abstract=2241536

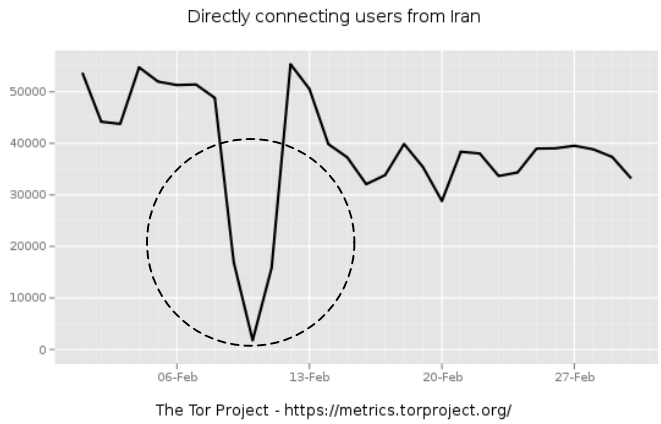


Figure 28 Drop down and rise in counts of directly connecting users from Iran across February 2012

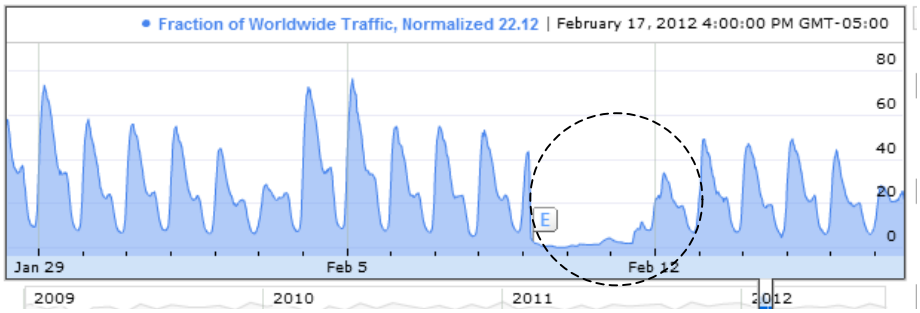


Figure 29 Drop down and rise of traffic from Iran to Google's Gmail encrypted service across February 2012

Figure 30 summarizes the action/reaction chain of events that we depicted in the three episodes above. We introduce a new actor, the Tor Project, as a nonprofit entity based outside the jurisdiction of Iran.

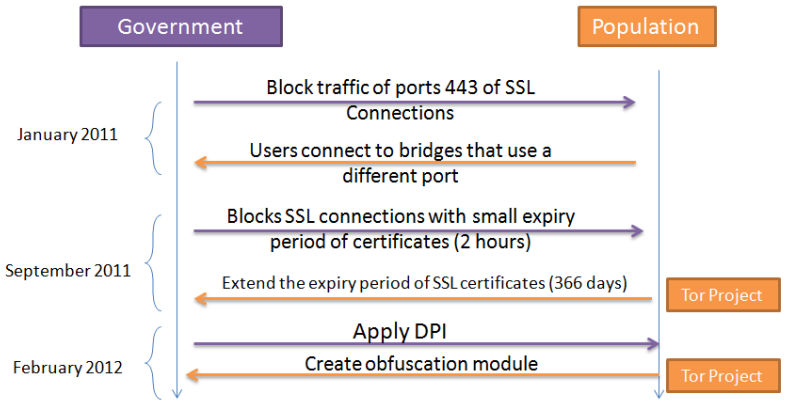


Figure 30 Late action/reaction chain in Iran in 2011-2012

The case of Iran raises several interconnected questions. How far is the Iranian government willing to increase censorship measures? How does that relate to architecture of the national network? What is the operational threshold of efforts exerted to control the speech of Iranians online? The British newspaper, *The Guardian* reported on January 2012 (before the third blockage "experiment") that the government seeks to substitute access to the global Internet with a National Intranet to provide a more controlled environment of communications in Iran (35). The expected Intranet model would also require that outside visitors obtain permission to view a site hosted within the cyber-boundaries of Iran, and for visitors from Inside Iran to obtain require permission to visit websites hosted on the global Internet.

Electronic copy available at: https://ssrn.com/abstract=2241536

Meanwhile, the Iranian government has formally requested that cybercafés would maintain records of national IDs and IP addresses of their Internet Users as well as visited sites IPs (35). By March 2012, the government required all Iranian citizens to register their websites with the Ministry of Culture[15]. The report of the *Guardian* relates the attempt to create a national Internet with the Stuxnet worm attack on Iran's nuclear project, which did have deep impacts on Iran's project (35).

Could this anticipated Intranet model create a sphere for some type of Internet and/or anonymity black market? If the Intranet model takes place, we do expect some entities to have more freedom than others in accessing the Global Internet (such as major businesses, Airports and Stock Exchanges). It might be reasonable to anticipate an ethical hazard where individuals leak access to global Internet illegally. Would proxy technology remain the sole enemy of the Intranet hopes because it is the only way that can enable "smuggling" of information from and to the Global Internet without the attention of government authorities? And do proxy technologies serve as functional equivalents to underground tunnels as challenges to cyber boundaries or jurisdiction?

V. CONCLUSION AND FUTURE RESEARCH

Anonymity networks are artifacts of the Internet. They enable citizens bypass their governments' "law enforcement"[16] (36) Therefore, they can be seen as a new arena for interaction between the protesters and their governments. More importantly, they have managed to threaten the political stability and security of several states.

This paper explored two cases of censorship where individuals effectively bypassed the censorship "wall" imposed by their governments. By illustrating the particular actions and reactions performed by each actor in these events, we could highlight the critical features of the escalation dynamics in these interactions. The key actions or events can be ranked from low to high severity as follows:

1. Block specific web sites in general (or in times of crises).
   -People respond by resorting to various proxy networks.
2. Block port 443 connections with the assumption that they are HTTPS connections.
   -People respond by using different port for HTTPS communications across Tor relays.
3. Distinguish Tor traffic by blockage of SSL connections with short-period SSL certificates.
   -Tor engineers respond by modifying the software to issue long-timed SSL certificates.
4. Apply Deep Packet Inspection on Internet Traffic to distinguish and block packets that are SSL encrypted or that include specific words such as "Tor".
   -Tor Engineers respond by creating obfuscation module to create ambiguity for the DPI classification algorithm. Still in test.
5. "Shutdown" the Internet across the nation.
   -In Egypt, such action aggravated the political stability of the country and did not mitigate the intensity of the demonstrations.

From political perspective, new actors have been empowered and taken on decision making roles that would have not been possible without the cyber-anonymity sphere. In the traditional world engaging in "illegal activity" was a major challenge in both theory and practice – being free speech under a repressive regime or a criminal activity- while maintaining anonymity. Governments suppressed such behaviors by physical search, physical security checkpoints, and prosecuting physical sources of information. Anonymous networks, however, have created another venue for practicing the same activities with even more freedom than before. Governments initially expected traditional control concepts of the physical space to be effective in the cyberspace, a space that is increasingly contested by various types of non-governmental actors.

[15] The Government of Iran Site to register sites owned by Iranians (Samandehi): http://www.samandehi.ir

[16] Dr. Joseph S. Nye refers to a similar idea in his book "The Future of Power" that: "diffusion of power away from governments - *is* one of the great power shifts in this century", as mentioned in his article "Cyberspace Wars", New York Times.

Electronic copy available at: https://ssrn.com/abstract=2241536

The dynamics that we explored in this paper can be seen as intersections of the spheres of influence among four different types of actors: Individuals, groups, governments and non-profit organizations,

a. **Individuals**: *acquire* the capacity to bypass government censorship of specific websites.
b. **Individuals**: *extend* this capacity to other individuals to preserve their online anonymity. This feature may well be specific to the very few networks like Tor network since Internet users across the globe can donate their machines and bandwidth to empower the Tor network -- even though the number of relays can affect the performance negatively if it exceeds a specific threshold (37).
c. **Governments**: *enforce* their authority of control, attribution and retribution on the cyberspace; that which has been undermined by the complexity, openness, decentralization and almost randomness of cyber anonymity venues, mainly the Tor network as well as many other anonymity tools[17] (38).
d. **Non-Profit Organizations**: *develop* and *support* anonymity networks; namely: Tor Project, I2P Network and a variety of anonymity networks that provide protection to the identity of individuals, journalists[18] (39), and in the same way, criminals[19] (40).

Anonymity networks are subject to all the usual vulnerabilities of the Internet. The case of Iran epitomizes the flaws, but also the developments, in the design of the Tor network that proceed from purely technical aspects of the Internet and that allowed the Iranian government to distinguish traffic to and from Tor network with advancing levels of accuracy. Further, other vulnerabilities discovered by various computer security research groups does not guarantee that they are the only existing vulnerabilities. Are there more? And *who* knows about them and can *act* based on that knowledge?

5.1 Future research

This exploratory inquiry suggests some new types of investigations:

First: *Can we anticipate or even forecast, certain political events based on metrics of cyber behavior*: The data sources in this paper include: BBC News, Google Trends, Google Transparency Reports, and Tor Project Metrics.

We related events on the ground (reported via news sources, mainly BBC News) and spikes in any of the behaviors of the various cyber-metrics we are using (Tor and Google). Previous work has been done in correlating quantitative data with events on the ground. Google has issued a paper on attempts to forecast several economic activities by applying regression models on Google Trends. The attempt is demonstrated forecasting of specific economic activities such as Home Sales, Automotive Sales, Travel and Retail Sales. Researching a similar approach (supported by computational modeling and optimization approaches) can result into a method for forecasting events on the ground based on the cyber behavior of the metrics deployed in this research.

Second: *Can we engage in Control Point Analysis of the Tor network*: David Clark (41) developed concept of Control Point Analysis with applications to illustrate its implications (3). Developing a Control Point model of the Tor network can help better understand, or even forecast the trajectory of the evolution of anonymous networks. Even with an initial assessment based on our investigations so far, we can anticipate that anonymous networks change over time.

1) Private–Public relations: Considering ISPs as main actors in censorship enforcement while being mostly private sector actors, what networks research tells about how much ISPs can influence anonymity would impact the dynamics of governmental relations with ISPs.

[17] FBI has closed an investigation on Aug 2, 2012 about a reported Child Pornography Site hosted on Tor Hidden Services. The final report entailed FBI's failure and "there is not currently a way to trace the origin of the website".
[18] Reporters Sans Frontières (RSF) has issued a guide for reports to educating them about the several types of proxy networks and proxy services that can help them hide their identity while working from countries with repressive regimes "Handbook for Bloggers and Cyber-Dissidents"

[19] "Silk Road" is an infamous example of a Tor-based criminal activity. It is an "ebay" for drug dealing. Recent study by Nicolas Christin evaluates the amount of revenue produced via this service to reach $1.9 million per month. This activity is based on Tor Hidden Services which is a mechanism to provide anonymity for web servers.

Electronic copy available at: https://ssrn.com/abstract=2241536

2) International Relations: Due to a) global nature of cyberspace and b) threats that anonymity can impose for both state's security and political stability, nations that are likely to be more "in control" of anonymity are also likely to maintain a considerable point of influence. This analysis can show that nations vary in power when it comes to undermining online anonymity.
3) Cooperation among nation states in order to undermine particular anonymity network can also change the whole view of integrity of anonymous networks and may even push other actors (being individuals, NGOs or governments) to develop stronger networks to overpower inter-state cooperation.
4) Tor engineers and researchers often referred in at least one of their recorded speeches to emergence of an "arms race" particularly with the government of Iran and the government of China (42) (which has employed stronger efforts into blockage of Tor network in China). This notion should stimulate skeptics as to: who really are the sides of this "arms race"? And how does it fit in the perspective of the traditional security dilemma introduced by John H. Herz (43)?

Therefore, an important next step for investigating the role and impacts of anonymity networks is to explore the synergy between the Control Point Analysis, International Relations levels of analysis (3) as well as the various technical properties of anonymity networks in computer networks and computer security domains.

Electronic copy available at: https://ssrn.com/abstract=2241536

VI. APPENDIX I: TOR DATABASE

The following is reproduced from Tor Project about the Description of the data required for relay servers to provide for the directory authorities (44):

***Server Descriptors**: We assume that the majority of server descriptors are correct. But when performing statistical analysis on server descriptors, one has to keep in mind that only a small subset of the information written to server descriptors is confirmed by the trusted directory authorities. In theory, relays can provide false information in their server descriptors, even though the incentive to do so is probably low.*

The following data fields in server descriptors may be relevant to statistical analysis:

- ***IP address and ports:** Relays provide their IP address and ports where they accept requests to build circuits and directory requests. These data fields are contained in the first line of a server descriptor starting with router. Note that in rare cases, the IP address provided here can be different from the IP address used for exiting to the Internet. The latter can be found in the exit lists produced by Tor Check as described in the Tor Check exit lists section below.*
- ***Operating system and Tor software version:** Relays include their operating system and Tor software version in their server descriptors in the platform line. While this information is very likely correct in most cases, a few relay operators may try to impede hacking attempts by providing false platform strings.*
- ***Uptime:** Relays include the number of seconds since the last restart in their server descriptor in the uptime line.*
- ***Own measured bandwidth:** Relays report the bandwidth that they are willing to provide on average and for short periods of time. Relays also perform periodic bandwidth self-tests and report their actual available bandwidth. The latter was used by clients to weight relays in the path selection algorithm and was sometimes subject to manipulation by malicious relays. All three bandwidth values can be found in a server descriptor's bandwidth line. With the introduction of bandwidth scanners, the self-reported relay bandwidth in server descriptors has become less relevant.*
- ***Relay family:** Some relay operators who run more than one relay organize their relays in relay families, so that clients don't pick more than one of these relays for a single circuit. Each relay belonging to a relay family lists the members of that family either by nickname or fingerprint in its server descriptor in the family line.*
- ***Exit policy:** Relays define their exit policy by including firewall-like rules which outgoing connections they reject or accept in the reject and accept lines.*

These are just a subset of the fields in a server descriptor that seem relevant for statistical analysis. For a complete list of fields in server descriptors, see the directory protocol specification.

Every hour, the directory authorities publish a new network status that contains a list of all running relays. The directory authorities confirm reach ability of the contained relays and assign flags based on the relays' characteristics. The entries in a network status reference the last published server descriptor of a relay.

The network statuses are relevant for statistical analysis, because they constitute trusted snapshots of the Tor network. Anyone can publish as many server descriptors as they want, but only the directory authorities can confirm that a relay was running at a given time. Most statistics on the Tor network infrastructure rely on network statuses and possibly combine them with the referenced server descriptors. The document below shows the network status entry referencing the server descriptor above. In addition to the reachability information, network statuses contain the following fields that may be relevant for statistical analysis:

- *Relay flags: The directory authorities assign flags to relays based on their characteristics to the line starting with s. Examples are the Exit flag if a relay permits exiting to the Internet and theGuard flag if*

Electronic copy available at: https://ssrn.com/abstract=2241536

a relay is stable enough to be picked as guard node

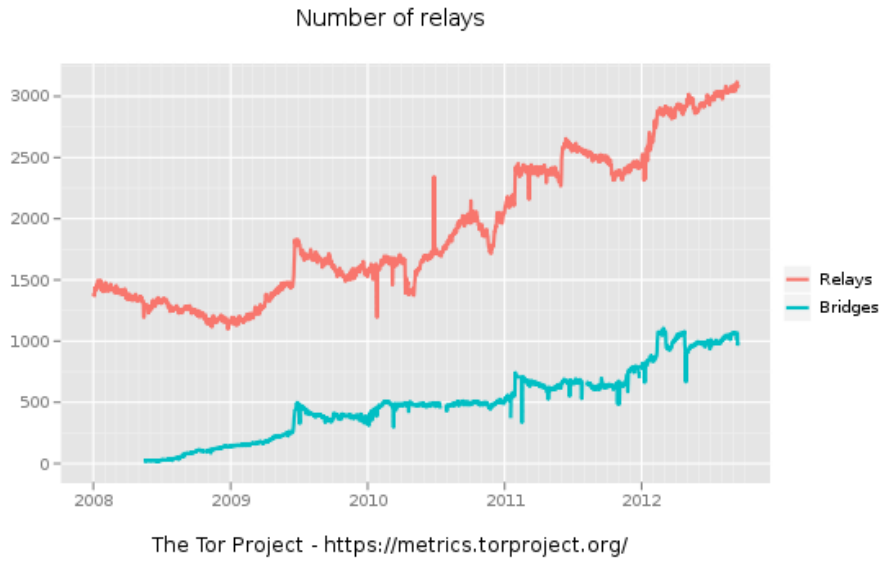
- *Relay version: The directory authorities include the version part of the platform string written to server descriptors in the network status in the line starting with v.*
- *Bandwidth weights: The network status contains a bandwidth weight for every relay in the lines with w that clients shall use for weighting relays in their path selection algorithm. This bandwidth weight is either the self-reported bandwidth of the relay or the bandwidth measured by the bandwidth scanners.*
- *Exit policy summary: Every entry in a network status contains a summary version of a relay's exit policy in the line starting with p. This summary is a list of accepted or rejected ports for exit to most IP addresses.*

Electronic copy available at: https://ssrn.com/abstract=2241536

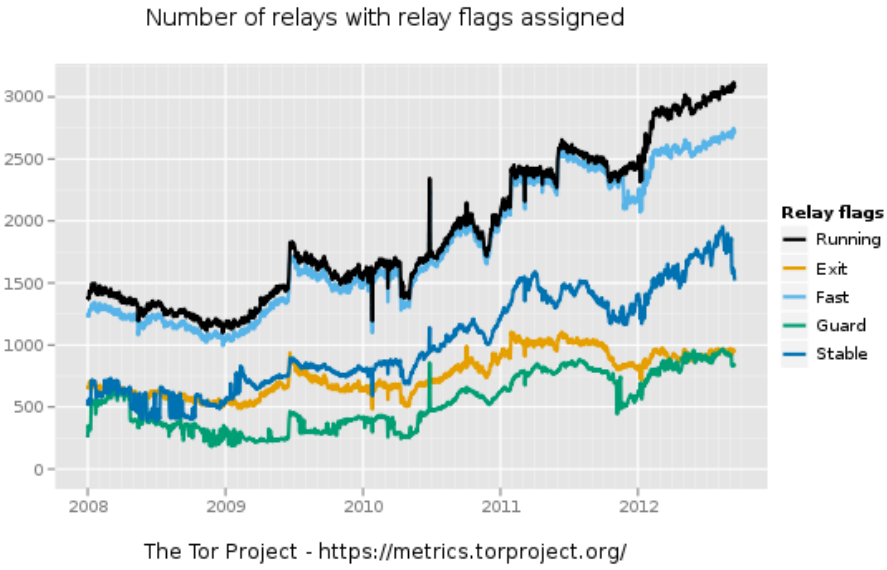
Appendix II: Graphs

Other Tor statistical Graphs (45):

a. Growth in number of relays vs. number of bridges.

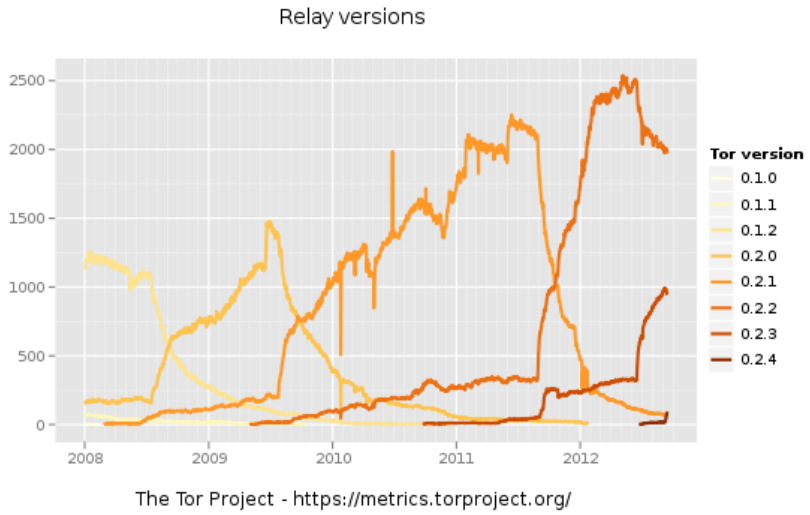


b. Statistics of Relays by status (Running/Exit/Fast/Guard/Stable):

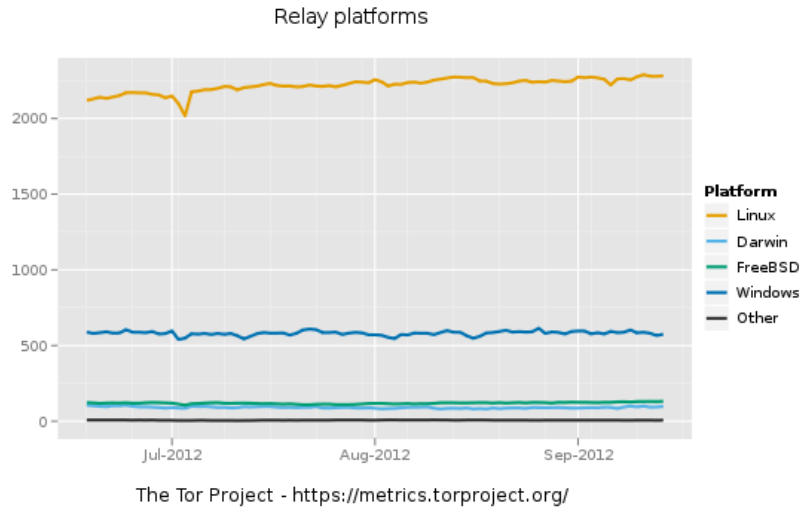


c. Version of Tor software running on each relay:

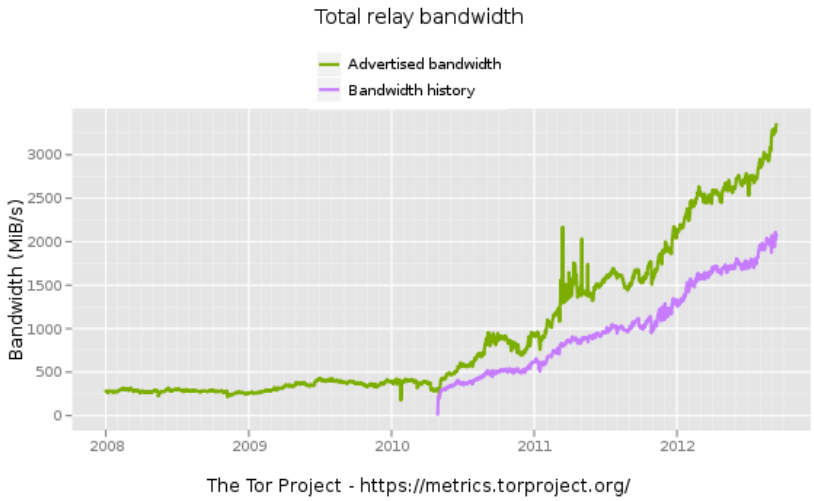
Electronic copy available at: https://ssrn.com/abstract=2241536



d. Platform of Tor relays (Open Source dominated):

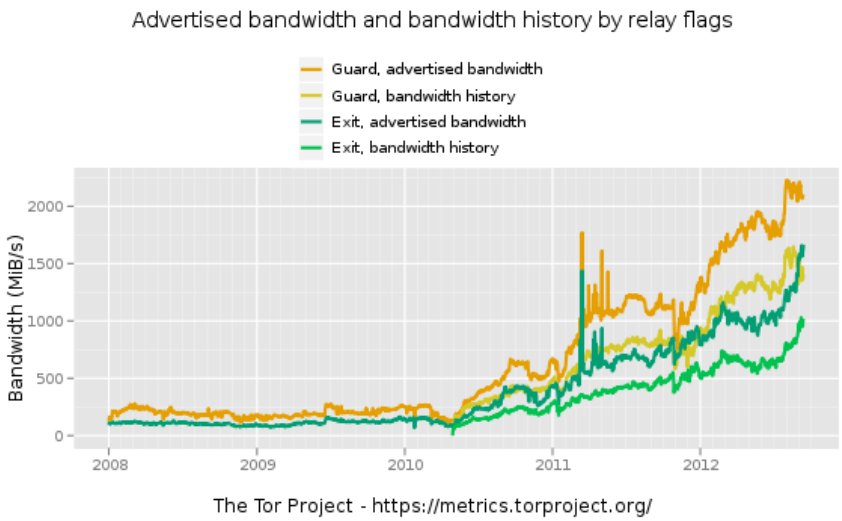


e. Relay bandwidth in the Netwoek (Advertised bandwidth Vs. tested/historical bandwidth)



f. Advertised bandwidth versus tested/historical bandwidth of relays by relay type:

Electronic copy available at: https://ssrn.com/abstract=2241536



Electronic copy available at: https://ssrn.com/abstract=2241536

REFERENCES

1. **Clark, David D. and Landau, Susan.** Untangling Attribution. *Harvard National Security Journal.* [Online] 2011. http://harvardnsj.org/wp-content/uploads/2011/03/Vol.-2_Clark-Landau_Final-Version.pdf.

2. **Zittrain, Jonathan.** Freedom and Anonymity: Keeping the Internet Open. *Scientfici American.* [Online] February 24, 2011. http://www.scientificamerican.com/article.cfm?id=freedom-and-anonymity.

3. **Choucri, Nazli and Clark, David.** Cyberspace and International Relations Toward and Integrated System. *Explorations in Cyber International Relations Project.* [Online] August 2011. http://ecir.mit.edu/images/stories/Salience%20of%20Cyberspace%208-25.pdf.

4. **Loesing, Karsten.** Measuring the Tor Network from Public Directory Information. *The Tor Project.* [Online] https://metrics.torproject.org/papers/hotpets09.pdf.

5. Configuring a Tor relay. *Tor Project.* [Online] https://www.torproject.org/docs/tor-doc-relay.html.en.

6. Tor FAQ. *Tor Project.* [Online] https://www.torproject.org/docs/faq.html.en.

7. Configuring a Bridge Relay. *The Tor Project.* [Online] https://www.torproject.org/docs/bridges.html.en.

8. **Hahn, Sebastian and Loesing, Karsten.** Privacy-preserving Ways to Estimate the Number of Tor Users. *The Tor Project.* [Online] November 30, 2010. https://metrics.torproject.org/papers/countingusers-2010-11-30.pdf.

9. **Loesing, Karsten.** Overview of Statistical Data in the Tor Network. *The Tor Project.* [Online] March 14, 2011. https://metrics.torproject.org/papers/data-2011-03-14.pdf.

10. **Danezis, George.** An anomaly-based censorship-detection system for Tor. *The Tor Project.* [Online] September 9, 2011. https://metrics.torproject.org/papers/detector-2011-09-09.pdf.

11. **Loesing, Karsten.** Case study: Learning whether a Tor bridge is blocked by looking at its aggregate usage statistics. *The Tor Project.* [Online] September 15, 2011. https://metrics.torproject.org/papers/blocking-2011-09-15.pdf.

12. Enemies of the Internet. *Reporters Without Borders.* [Online] March 11, 2012. http://en.rsf.org/china-china-12-03-2012,42077.html.

13. China's Profile. *Open Net Initiative.* [Online] August 09, 2012. http://opennet.net/research/profiles/china.

14. "Clashes in Egypt strike stand-off". *BBC News.* [Online] April 6, 2008. http://news.bbc.co.uk/2/hi/middle_east/7332929.stm.

15. "Egyptians hit by rising food prices". *BBC News.* [Online] March 11, 2008. http://news.bbc.co.uk/2/hi/middle_east/7288196.stm.

16. "Egypt strike fails to make impact". *BBC News.* [Online] May 4, 2008. http://news.bbc.co.uk/2/hi/middle_east/7382598.stm.

17. Alexandria church bomb: Egyptian Copts and police clash. *BBC News.* [Online] January 2, 2011. http://www.bbc.co.uk/news/world-middle-east-12106177.

18. Live: Tunisia turmoil a day after fall of Ben Ali. *BBC News.* [Online] January 15, 2011. http://news.bbc.co.uk/2/hi/africa/9362712.stm.

19. About Google Trends. *Google.* [Online] 2011. http://www.google.com/intl/en/trends/about.html#9.

20. **El Deeb, Sarah.** Egypt Porn Ban: Court Orders Censorship Of Pornographic Websites. *Huffington Post.* [Online] March 29, 2012. http://www.huffingtonpost.com/2012/03/30/egypt-porn-ban_n_1390836.html.

Electronic copy available at: https://ssrn.com/abstract=2241536

21. Salafist MP demands Egypt ban on porn sites. *Ahram Online.* [Online] February 20, 2012. http://english.ahram.org.eg/NewsContent/1/64/34976/Egypt/Politics-/Salafist-MP-demands-Egypt-ban-on-porn-sites.aspx.

22. **Wolchove, Natalie.** Egypt unrest: How do you shut down Internet service in an entire country? . *The Christian Science Monitor.* [Online] January 28, 2011. http://www.csmonitor.com/Science/2011/0128/Egypt-unrest-How-do-you-shut-down-Internet-service-in-an-entire-country.

23. False Freedom, Online Censorship in the Middle East and North Africa. *Human Rights Watch.* [Online] 2005. http://www.hrw.org/reports/2005/mena1105/5.htm#_ftn165.

24. Iranian blogger imprisoned for two years 'sentence'. *BBC News.* [Online] June 7, 2005. http://www.bbc.co.uk/persian/iran/story/2005/06/050606_sm-madyar.shtml.

25. **Boyd, Clark.** Iran targets dissent on the net. *BBC News.* [Online] June 24, 2005. Iran targets dissent on the net.

26. EDITORIAL: Iran's Twitter revolution. *The Washington Times.* [Online] June 16, 2009. http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/.

27. **Shachtman, Noah.** Activists Launch Hack Attacks on Tehran Regime. *Wired.* [Online] June 15, 2009. http://www.wired.com/dangerroom/2009/06/activists-launch-hack-attacks-on-tehran-regime/.

28. Young Iranians use video to tell story. *BBC News.* [Online] June 16, 2009. http://news.bbc.co.uk/2/hi/middle_east/8102676.stm.

29. Core Tor People. *Tor Project.* [Online] https://www.torproject.org/about/corepeople.html.en.

30. New Blocking Activity from Iran. *The Tor Project Blog.* [Online] Jan 9, 2011. https://blog.torproject.org/blog/new-blocking-activity-iran.

31. Iran blocks Tor; Tor releases same-day fix. *Tor Project Blog.* [Online] September 14, 2011. https://blog.torproject.org/blog/iran-blocks-tor-tor-releases-same-day-fix.

32. Iran temporarily blocks Internet access. *The Computer Business Review.* [Online] February 14, 2012. http://www.cbronline.com/news/iran-temporarily-blocks-encrypted-internet-access-140212.

33. Iran partially blocks encrypted network traffic. *Tor Project Blog.* [Online] February 10, 2012. https://blog.torproject.org/blog/iran-partially-blocks-encrypted-network-traffic.

34. Obfsproxy: the next step in the censorship arms race. *The Tor Project Blog.* [Online] February 16, 2012. https://blog.torproject.org/blog/obfsproxy-next-step-censorship-arms-race.

35. **Dehghan, Saeed Kamali.** Iran clamps down on internet use. *The Guardian.* [Online] January 5, 2012. http://www.guardian.co.uk/world/2012/jan/05/iran-clamps-down-internet-use.

36. **Nye, Joseph.** Cyberspace Wars. *The New York Times.* [Online] February 27, 2011. http://www.nytimes.com/2011/02/28/opinion/28iht-ednye28.html.

37. What if the Tor network had 50,000 bridges? *Tor Project.* [Online] March 9, 2012. https://metrics.torproject.org/papers/bridge-scaling-2012-03-09.pdf.

38. 'Dark Net' keeps FBI from investigating child porn. *NBC News.* [Online] June 14, 2012. http://www.msnbc.msn.com/id/47815897/ns/technology_and_science-security/t/dark-net-keeps-fbi-investigating-child-porn/#.UFPDuY1mREM.

39. **Villeneuve, Nart.** Technical Ways to Get Round Censorship. *Handbook For Bloggers and Cyber-Dissidents.* s.l. : Reporters Without Borders, 2005.

Electronic copy available at: https://ssrn.com/abstract=2241536

40. **Christin, Nicolas.** Traveling the Silk Road:A measurement analysis of a large anonymous online marketplace. *Carnegie Mellon Cylab.* [Online] July 30, 2012. http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf.

41. **Clark, David.** Control Point Analysis. *Social Science Research Network.* [Online] September 10, 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2032124.

42. **Hung, Shirley.** The Chinese Internet: Control Through the Layers. *ECIR Project.* [Online] October 30, 2012. http://ecir.mit.edu/images/stories/Hung_Internet.pdf.

43. **Herz, John Z.** The Security Dilemma in International Relations: Background and Present Problems. *World Politics.* 1950, Vol. 2, 2.

44. Tor Metrics Portal: Data Formats. *Tor Project.* [Online] https://metrics.torproject.org/formats.html.

45. Tor Metrics Portal: Network. *Tor Project.* [Online] https://metrics.torproject.org/network.html.

46. "Confusion over Egyptian blocks on web protest tools". *BBC News.* [Online] January 26, 2011. http://www.bbc.com/news/technology-12291982.

47. **Choucri, Nazli.** New Challenges to International Relations Theory and Policy. *CyberPolitics in International Relations.* 2012.

48. Net firms criticised over China. *BBC News.* [Online] February 15, 2006. http://news.bbc.co.uk/2/hi/technology/4699242.stm.

49. Timeline: China's net censorship. *BBC News.* [Online] June 29, 2010. http://www.bbc.co.uk/news/10449139.

50. Google Transparency Report. *Google.* [Online] August 10, 2012. http://www.google.com/transparencyreport/traffic/?r=IR&l=YOUTUBE&csd=1326580960318&ced=1332476228509.

51. Youtube. *Copyright Center.* [Online] http://www.youtube.com/t/copyright_my_video.

52. Wikipedia Procedural Policy:Open proxies. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Wikipedia:Open_proxies.

53. Egypt internet comes back online. *BBC News.* [Online] February 2, 2011. http://www.bbc.com/news/technology-12346929.

54. *How governments have tried to block Tor* . http://www.youtube.com/watch?v=GwMr8Xl7JMQ&feature=related.

55. *Technology and Internet Jurisdiction.* **Reidenberg, Joel R.** 2005, s.l. : University of Pennsylania Law Review, Vol. 153.

Electronic copy available at: https://ssrn.com/abstract=2241536