THE DICTATOR'S PRACTICAL INTERNET GUIDE TO POWER RETENTION

Global Edition

by Laurier Rochon
email : l@pwd.io

text available at : http://pwd.io/guide
June 2012, Rotterdam, The Netherlands

1. Objective of this guide

The goal of this guide is to provide leaders of authoritarian, autocratic, theocratic, totalitarian and other single-leader or single-party regimes with a basic set of guidelines on how to use the internet to ensure you retain the most power for the longest time.

The best way to achieve this is to never have your authority contested. This guide will accompany you in the obliteration of political dissidence. By having everyone agree with you, or believe that everyone agrees with you, your stay at the head of state will be long and prosperous.

As non-democratic regimes come in incredibly varied flavors, some of the formulated recommendations will be of greater relevance for some dictators than others, depending on a long list of factors pertaining to the state you rule. Generally, states with higher economical growth rates have easier choices to make.[58] This guide will attempt to cover as much ground as possible, but aims first and foremost to offer general advice.

Authoritarian values are being attacked in all parts of the world, and dictators use merely a fraction of the internet's capabilities when it comes to controlling their population. This can be partly attributed to the effectiveness of traditional repressive techniques, the misguided belief that technology has inherent democratic properties or the lack of interest in developing a strong tech culture. Leaders of non-democratic states need to change their mindsets and better adapt to this new landscape overflowing with opportunities.

As you will see, some of them are not without risks, but the rewards to be reaped are immense and the possibilities, nearly endless.

Contrary to popular belief, technological development does not automatically translate into more democratic institutions. Many authoritarian countries which have experienced steady or rapid degrees of ICT diffusion have happily stayed authoritarian, namely Brunei, Eritrea, Gambia, Iran, Jordan, Morocco, Oman, Russia and others.[59] This guide aims to distill common threads and useful practices in order to emulate the success some of these states have achieved.

2. Essential conditions: three freedoms

In order to derive maximum benefit from the internet, you absolutely must fulfill three prerequisites. As you will see in the next chapter, they are essential to successfully disable anonymity and security, your two greatest threats. These freedoms will enable you to exercise control mechanisms effectively, safely and often at relatively low cost. There are undeniable advantages (economic, political and social) and many collateral gains associated with successful implementation of the following recommendations and it is vital for your despotic reign to take these prerequisites very seriously.

2.1 Freedom from political chaos

Firstly, the country you rule must be somewhat “stable” politically. Understandably “stable” can be defined differently in different contexts. It is essential that the last few years (at least) have not seen too many demonstrations, protests questioning your legitimacy, unrest, political dissidence, etc. If it is the case, trying to exploit the internet to your advantage can quickly backfire, especially if you can’t fully trust your fellow party officials (this is linked to condition #3). Many examples of relatively stable single-leader states exist if in need of inspiration, Fidel Castro’s Cuba for example. Castro successfully reigned over the country for decades, effectively protecting his people from counter-revolutionary individuals. He appointed his brother as the commander in chief of Cuba’s army and managed his regime using elaborate surveillance and strict dissuasive mechanisms against enemies of the state.[49] As is always the case, political incidents will occur and test your regime's resilience (the Bay of Pigs invasion or the missile crisis, for example), but even massive states have managed to uphold a single-party model and have adapted beautifully to the digital age - in China's case, despite close to 87 000 protests in 2005.[2] Follow these states' example and seek stability, no matter what your regime type is. Without it, you are jeopardizing the two next prerequisites and annihilating your chances to rule with the internet at your side. If you are in the midst of an important political transformation, busy chasing counter-revolutionary dissidents or sending your military to the streets in order to educate protesters, you will need to tame these fires first and come back to this guide afterwards.

2.2 Freedom from decentralized telecommunication infrastructure

Most countries already possess the infrastructure to support the internet, at least to some degree. Regardless of that degree, you must ask yourself some important questions: who owns the fiber-optic cables that run through your country? Where are your most important data centers located? How safe are they (both physically and digitally)? Do you have major hubs of traffic control? Who owns these hubs? Does your government have enough trained professionals to operate this infrastructure?

The answers to these questions should help you assess whether you have sufficient control over your infrastructure to go forward or not with implementing the strategies of this guide. You must have either direct executive power or overwhelming influence over all parts of the internet supply chain, including hubs connecting to other countries, cables within your country, domestic traffic hubs, and internet service providers and their parent companies.

You must be in a position to pull the plug if necessary, to black out cyberspaces (a website, word collections, search terms, servers) just as easily as physical spaces (a neighborhood, a province, a company). Just a few hours before the polls opened for voting at the 2009 elections in Iran, "text messaging went dark, [...] key opposition websites went offline. The government began jamming the frequencies of Farsi-language satellite broadcasts from the BBC and Voice of America as well".[53] Having to negotiate with the owner of a network to obtain certain favors is not an option. You are the mainframe and all child processes obey your command.

Unfortunately, it will be difficult in some cases to have perfect control of all infrastructure due to varying factors (multiple telecommunications providers, political and structural legacy from past regimes). Russia and China, which represent massive geographic areas, face this challenge. Although they have adopted different approaches, these two countries have nonetheless managed to compound convincing physical ownership with strong legislative ordinances and heavy government oversight in digital affairs. Regardless of how it is done, make sure you always have your internet's switch at the tip of your fingers.

2.3 Freedom from democratically elected officials

Whether the Minister of Public Safety, Minster of Internal Affairs or a special appointed officer to digital matters is responsible for making up the rules regarding the how, what and when of internet service to citizens, be sure you can trust this person like none other. In a best case scenario, appoint a family member to this position or an old friend who would rather die than turn his back on you. The same rule applies to whoever runs all internet Service Providers (ISP) in the country, as they will have to work with your appointed official on digital matters daily. Make sure these people are reliable and loyal, give them all the resources they need and make sure to weed out any dissidence, internal corruption or other sources of potential friction within these organizations. As Philip N. Howard maintains, elite defection usually marks the end of an authoritarian regime.[50] Make sure this regime isn't yours.

Along with your army's leader, this is certainly one of the last areas of control you will want to surrender. Most ISPs, for historical reasons, have grown out of telecom providers (often, adapting telephone infrastructure to internet infrastructure was not a big issue), which are often state-funded and controlled. Therefore, they are the gateway to what your population knows, how they know it, where they reach out to get information and how they organize. Keeping a strong grip on ISPs and telecom providers is paramount to your success, as history has taught us that carrying a big violent stick can work well, but being the guardian of the collective consciousness is usually a much more sustainable evil.

If you are not in a position to fulfill these prerequisites...

The wisest path to follow is to temporarily ban the open internet as aggressively as possible and simply stay off the grid, as North Korea is currently doing.[5] However, it is important to quickly adapt to this new reality and make the necessary changes to meet these aforementioned requirements. Even North Korea will eventually have to open up. Its obsession with staying in the 20th century cannot last indefinitely while the rest of the despotic world marches on towards technological victory.

3. Creating optimal surveillance conditions

There are two things that are simply not compatible with the regime you run: anonymizing tools and data-encrypting tools. With anonymizing tools, you can perhaps control and monitor internet activity, but you cannot tie this activity to a certain individual. Anonymity thus makes accountability evaporate. With data-encrypting tools, you cannot even see or make sense of the data which travels in the internet cables you control, as it is mangled specifically to avoid being recognizable. The proliferation of online political dissidence in non-democratic states is usually dependent on the availability of tools to anonymize and encrypt data. If you cannot effectively dismantle the use of these tools, it's often a matter of (short) time before political opposition organizes against you.

3.1 Suppressing anonymity (who)

Proxies

It is crucial to understand how anonymizing and encrypting tools work in order to ensure they never reach your citizens. There are numerous applications that can render a user anonymous when connected to the internet, but most function in a similar manner. Internet proxies pose the most serious threats in this area and will be dealt with in this section, in particular one project called "Tor".

It's an easy matter to link an individual's activities to his or her internet Service Provider's account [note 1]. But if this individual wants to connect anonymously to a site without your honorable consent, he can ask another computer to do it for him - masking his own identity. This intermediate server is called a proxy, as it allows people to connect to “in-between” computers to maintain their anonymity. This “in-between” computer will then fetch the information requested and send it back like a messenger. Retrieving documents through proxies is popular in dissident circles as it allows them to operate under your watchful radar.

What can be done against such vile circumvention techniques? First, good proxies often become victims of their own popularity. If a proxy is effective, an obvious surge in traffic to an unknown computer will appear, which should be investigated promptly. Stay alert to such spikes and add any new proxy to your blacklist. Second, set up your own proxy servers! Most people connecting to proxies are not technologists, they simply want access to resources that are kept from them. Many assume that proxy providers could only be the product of a “free”, “democratic” mind and simply assume they are not monitored. Let your state-owned proxy get through banning filters and collect all the information about those taking advantage of it. Then crack down on them (by then you can have physical addresses) and make a major public case out of it. Let your citizens know that you are tech-savvy and setting up your own proxy servers, which should discourage them from ever using them again.

The Tor Project

A second, more recent and more dangerous threat to watch out for is called “Tor”. Tor is a bundle that comprises of a large network of nodes run by users - which essentially act as proxies - and custom software built to take advantage of this network. The way that Tor distinguishes itself from a normal proxy is fairly simple. Tor is more or less a large network or many intelligent proxies that can communicate with each other. Tor makes possible multiple proxy jumps through these “relays” while carrying only parts of the data to be sent back. This makes it much more complicated to track who is requesting what, as no single node on the network will show a large spike of traffic and each node is only aware of its previous/next jump and none of the others. Furthermore, Tor nodes can quickly crop up and go down unlike monolithic proxies.

The sophistication of Tor has made many fellow dictators nervous in the last few years (and rightly so), but there is no need to panic. Again, there are solutions to address this problem. First, make sure to filter out, ban, remove and delete any mention of Tor on your network. This is the first and most important step to guarantee that Tor is simply invisible to your population. According to Tor’s statistics, no authoritarian country other than Iran has a significant user base.[23] Given that this solution is not exactly a “solution” but merely a precaution, you must prepare to fight fire with fire if Tor enters your country. Since Tor is decentralized and relies on unknown volunteers to grow its network, you should set up your own Tor relays, and carefully analyze the traffic flowing through them. Mobilize your cyber-army and hire new digital combatants as quickly as possible. By design, Tor is meant to protect transport of data within its network, but will never be able to control the entry and exit points of this data [note 2]. Focus on these two areas to gather data [note 3]; by doing this, you might learn enough to precisely identify who is doing what.[24] Finally, learn more about the project, how it works, who contributes to it, what its internal mechanics are. It is free and open source, meaning that any of your highly skilled programmers can understand how it functions.

Lastly, a more general and perhaps more important thing to remember: while these techniques may seem to require heavy time and energy investments, you hold an undeniable edge as you create complications, introduce new procedural steps and impose this burden on proxy and Tor users to access simple resources anonymously. Tor grew out of a necessity to protect users' privacy and represented a big leap forward in doing so, but also added a new layer of complexity for non-technologists who want to use the internet anonymously. In time, many add-ons and extensions needed to be bolted onto Tor in order to satisfy particular needs [note 4]. As you fight these initiatives, tools become more and more complex to use, which at the end of the day, will discourage the average user who might simply want look up vaguely sensitive material.

3.2 Suppressing security (what)

A more serious problem than anonymity is likely data encryption, where you can tell that someone is requesting "something" but you cannot determine what. On the other hand, it is an easier problem to solve. There are many traffic types on the internet including peer-to-peer, http, VPNs, FTP, mail, etc. They all use different protocols to communicate data, and all possess different levels of security when transporting this data. For example VPNs (virtual private networks) are specifically designed to encrypt data, http can rely on https for encryption, and so on.

Ban or disable all forms of encrypted content. This certainly includes VPNs and other tunneling technologies. You simply cannot afford to be blind to what your citizens are doing online. Iran has acted wisely on this front, effectively blocking https traffic in February 2012.[25] Whenever possible, catch users off guard and monitor their behavior, while giving the impression they are safe. For example, there are ways to hack the https protocol while users are merely browsing their email or submitting login information on various sites (banks, social networks) [note 5]. Having access to their email, social networks and bank account extends your options to wherever your imagination can take you. In addition, force device makers and hardware companies to include back-door access to computer components, which you can tap into whenever needed. The next recommendation details this strategy further.

Remember, the point is not to block every single protocol that relies on the internet. Ideally you would block only a small minority of them, and let everyone else go about their business using unencrypted connections.

3.3 Run your own services

Given a more totalitarian regime, the "run-your-own" tactic is also commendable. This requires solid control of online distribution channels and heavy network interference but will provide you with near-perfect oversight of your citizens' activities. In collaboration with hardware and software developers, enforce exclusive back-door access to computers sold in your country (touched upon in the next chapter) and create software tailored to your needs. For example, a web browser that respects your URL blacklist, a virus scanner that detects digital threats (such as other non-authorized web browsers) or an email client that performs textual inspection when emails are sent and received. This strategy also includes distributing software such as Tor through unofficial channels (the original website must be banned), and adding malicious code to the package, allowing you to monitor people and their activities. You should also create a national operating system, which comes pre-installed on every personal computer, probably eliminating the need to create particular software packages. Of course this operating system could send detailed reports on usage, illicit activity and troves of other useful information back to your central surveillance entity.

Once you know who does what…

There should be no more secrets for you. With complete political power and enough human resources, you can monitor all bytes flowing through your internet cables and curate what people see and do without breaking a sweat. As Iran has done, build a simple choke point into your internet and proceed with deep packet inspection on all traffic flowing through it.[55] The next chapter of the guide deals with “variable tactics” to effectively control your population using the internet, after you’ve conquered anonymity and security. But first, a discussion on harnessing the full power of private industry will explain how a strong, docile tech industry can further assist you in your battle against anonymity and security while offloading a lot of your work to the private sector.

3.4 Harnessing private sector innovation

It’s possible to seal off your country completely to all new technology and be uncompromisingly severe on your control strategy - North Korea being the leading example once again. However, this is not recommended unless you are currently putting together the building blocks for your future internet. Such a strategy will eventually erode, then collapse. On the North Korean border with China, cellphone signals can be used to communicate with hand-held devices. As technology improves and devices capable of relaying wireless signals get better, this will only worsen. North Koreans have been caught smuggling South Korean cassette tapes and other goods across the border[6], and it’s only a matter of time before these cracks widen enough that people will want to know the truth which has been kept secret from them.

Depending on your regime’s size and power, it is possible to develop state-of-the-art internet infrastructure to serve your citizens, but to severely filter the data flowing through it, as it is done in some Islamic republics and constitutional monarchies.[61] Many of these regimes don’t mind curbing economic development in exchange for cultural capital, but not all states are oil-rich like Saudi Arabia, for whom such investments are insignificant. However, it is also possible to foster a thriving private tech industry and keep companies on a tight leash instead, as Singapore has done.[62]

3.4.1 Private industry

This could seem counterintuitive for many dictators running communist or socialist single-party states, but a thriving private tech industry can contribute invaluable tools to help you implement a controllable internet. The reason is fairly simple: the technologies that transform internet applications into more personalized, efficient and enjoyable experiences are usually the same ones that increase the capacity to monitor its users. While internet cookies have solved the problem of stateless servers, they are perfect for tracking users (and even sometimes hacking them).[8] Even though the internet's basic protocol (TCP/IP) is blind to what it carries and what its real-world destination is, clever programmers quickly built tools that can be layered on top to provide more detailed information. The result is a much more personalized experience (Websites shown in localized language, local currency when buying online, personalized search results to match local realities, targeted ads, etc.) but also tremendous potential to track what data is traveling when and where.[67]

Data tracking technology can only bring us to an IP address (what computers use to communicate with each other) which translates into a particular computer (or network of computers), not a person nor a reliable physical space. But if you've fulfilled prerequisite #3, this is no longer a problem. Having full control of your internet service provider is the key here, as they are the ones who allocate different subscribers (clients) their IP addresses. As demonstrated earlier (note 1) it is child's play to match an IP address' account holder with their online activity.

Once again, making your internet more efficient via private sector innovation has tremendous advantages: 1) you give a greater impression of impartiality, that government is not interfering in the development of important privacy-altering technologies; 2) these innovations provide you with a powerful arsenal of surveillance tools; 3) you provide your citizens with a richer, more enjoyable internet experience; and 4) you gain significant economic advantages by creating a new service industry. As Lawrence Lessig would say, “These changes [to the design of the internet] are not being architected by government. They are instead demanded by users and deployed by commerce.[...] Once again, commerce has come to the rescue of regulability.”[9]

The gains to be made from a booming tech economy should now be clearer. If the industry grows too quickly, flex your control muscle. Carefully massage your interests into the industry’s ecosystem by whatever means at your disposal. Soft techniques - such as subsidizing companies and new developments that enable better surveillance or tracking (competitors will not be in a position to compete) or creating legislation that favors these same companies (tax breaks, special privileges, etc.) - are often easily implemented. You can also force certain product makers to include surveillance mechanisms, as the German government was found to be doing in 2011 with its “staatstrojaner”, a computer virus deployed to watch over “suspected individuals”.[31] In the 1970s and 1980s, Libya required every computer to be registered with the government.[60] Moreover, in February 2012, Pakistan published a public tender “for the development, deployment and operation of a national-level URL filtering and blocking system.”[44], asking private companies to send in their proposals. Total project worth: $10 million. Were they concerned about public opinion or concealing their intentions? Apparently not - they even bought ads in newspapers to advertise the call for proposals. Do the same: encourage the growth of the surveillance industry via consumer products and regularly boast about how much your citizens are the technological cream of the crop. So-called “black box” technologies are currently thriving, as it becomes clear that technology users from around the world are willing to sacrifice transparency for a better user experience.

Your citizens need to be regulated, but you can have industry do much of the heavy lifting for you. Instead of creating draconian laws that will surely draw the ire of certain citizens, simply encourage a technology maker, enabling a similar end result. Examples of this from around the world are too numerous to list, as it has been standard practice since the internet’s inception. Every aspect of technology has been a recipient of this “selective preferential treatment” by governments, including a myriad of software, routers, data centers, security firms, social media tools and so much more. This strategy has been tested and proven for decades already, deployed by all types of regimes up to now. It’s a public relations gold mine and an unbeatable surveillance plan.

3.4.2 Localhost

According to Facebook, there are more users of its service in Ottawa, Canada’s quiet capital city and home to roughly one million, than in all of China, a country of over a billion inhabitants.[10] While this may sound improbable, it will make sense to those familiar with China’s aversion to internet services developed by Western states. Facebook has been banned in mainland China (while very popular in Hong Kong) since 2009 [11] and the government heavily censors or condemns others (Google’s Chinese site, for example, now redirects to its Hong Kong counterpart). Its strategy has been to prohibit tools which challenge the government’s legitimacy while creating national equivalents for its ordinary citizens. Chinese people can’t use Google, but they have Baidu. Facebook is banned, but RenRen offers a similar fix. Twitter is nowhere to be found, enter Weibo. All these spinoffs cannot rival their original counterparts from an engineering perspective, but it doesn’t matter: they don’t need to. As long as the experience is close enough to the original, there is not much for users to complain about (all these services are free). It might seem like replacing one evil with another, but there is a very fundamental difference that is often invisible to the user: the rulers of China can (and do) create legislation that supports their tough censorship policies, which companies from China must abide by. Additionally, China’s leaders can sleep much more soundly, knowing that its massive internet populations’ data resides within the borders of its country, and not somewhere near the sandy beaches of California, subject to American legislation.

Take advantage of the fact that often, online service providers adapt clumsily to new global markets. Exploit differences in religion, language and local customs to provide them with a personalized experience they can connect with - surely they will trust it more than a vanilla template designed for the masses. As long as the larger overarching system uses infrastructure you control, and is subject to legislation you have power over, the more people enroll in social and local internet services, the better. One of the most popular email services in China is actually Yahoo!, in part because it was founded by Chinese entrepreneur Jerry Yang, but also because it signed the “Public Pledge on Self-discipline for the Chinese internet Industry”. Sometimes, it is not even necessary to clone a popular western service as these companies will, once in awhile, do all the dirty work for you. In a best case scenario, online services should serve as a soft mouthpiece to gently enforce government policy.

At the time of writing, Russia, a world-renowned champion at numbing its internet users with “entertainment media” [68] is struggling with a political crisis that partly hinges on the use of an American website called LiveJournal. Because “its servers were in the US at a time when the Russian government was tightening the screw on private media, it was seen as a guarantee of freedom of speech”.[34]

The lessons to be learned from China and Russia are important: letting people chatter on micro-blogging services and social networks is harmless if you control these networks and monitor their contents. Even better, have these services depend on government resources, putting you one step closer to the data of its users.

3.4.3 Tools and intentions

In the summer of 2010, the Hackers On Planet Earth Conference (H.O.P.E) took place in New York City, with Julian Assange - the founder of Wikileaks, a website that lets whistleblowers submit secret documents - scheduled to give the keynote speech. This was barely two months after Wikileaks had released the leaked video “Collateral Murder” showing American soldiers gunning down journalists in Baghdad, and just before hundreds of thousands of other war documents were leaked (the Afghan War Diary and the Iraq War Logs). Assange didn’t show up for the keynote, probably for security reasons, as worldwide media coverage of the events was at its peak. In his place, security researcher Jacob Appelbaum took the podium and gave a speech about security, anonymity and the project that was keeping him busy at the time, Tor. As mentioned earlier, Tor “helps you defend against a form of network surveillance that threatens personal freedom and privacy".[13] Of course, rock-solid security plays an instrumental role for Wikileaks - at least if it wishes to protect its sources. Tor gained a lot of subsequent traction and Abbelbaum's work certainly made him a marked man in the United States. His Twitter updates testify to the hard time border and customs officials have given him when entering or leaving the country, including confiscating equipment and subjecting him to many interrogations. A status he tweeted on January 19 2011 read: "I'm looking forward to a time when I'm not on a secret watch, search, harass, detain, interrogate, delay, annoy and stress list."[12] The American government was throwing everything it had at Appelbaum. Obviously someone who worked hard to anonymize the identities of whistleblowers (who in this case, leaked data that was very embarrassing for the government) needed to be watched carefully.

During the next few months we witnessed the discontent of populations from middle eastern and northern African countries demanding more democratic states and calling for their leaders to either cede power or simply step down. These demands have stemmed from a mixture of slow processes (politicization, to name one), accumulated dissatisfaction (constant restrictions on freedom of speech, for example) and pivotal moments (Mohamed Bouazizi's immolation in Tunisia, for instance). I won't delve into these catalyzing elements here (I deal with how to (de)politicize your population later), but it's important to consider how internet technology might have aided in organizing, synchronizing and informing these populations about their own regime, upcoming local events, and so on. Even in countries like Iran, Egypt and Saudi Arabia, where censorship is swift and unforgiving, populations have managed to bypass certain governmental filters and remain anonymous, thanks to software like Tor! Hillary Clinton’s seminal speech in 2010 about internet freedom and its role in the democratization process echoed the demands of these states’ populations: “Information freedom supports the peace and security that provide a foundation for global progress. We need to put these tools in the hands of people around the world who will use them to advance democracy and human rights”.[14] It just so happens that the same piece of software the U.S government is severely condemning for its ability to anonymize its users could also be the cornerstone of new revolutions in non-democratic countries.

This short story about Tor, Wikileaks and American foreign policy should serve as a cautionary tale for all serious dictators. It is meant to illustrate how technologies, put in a different context, can wield incredibly different powers that will enable or disable your control strategy. It also shows how silencing technologists that currently work against you is not always the best stance to adopt. By creatively repurposing tools produced by your local tech industry, you can disguise your true intentions and more effectively control your citizens. Also, carefully ponder your options when faced with talented hackers and bright engineers (whether they are on your side or not, ideologically speaking), as they may believe in certain ideals (freedom of information, security, anonymity etc.) which will sometimes align with your government policies and sometimes not. When new technologies are being developed to undermine your regime, take the time to reverse engineer them, take them apart, try to imagine them for other uses, in other contexts, combined with other factors (which you might have great control over). Moreover, are the creator’s intentions primarily political or technological? Aided by competent engineers, such an attitude will tremendously increase both your offense (to implement your control strategy) and your defense (anticipating and fighting off your opponents).

4. Choosing a control strategy

4.1 Variable tactics

By suppressing anonymity and security you've put yourself in an enviable position. The internet is now an open, transparent book. The next step? Gather as much intelligence as possible: what is your population interested in? How are they using the internet? Are citizens streaming stand up comedy shows to relax after a long day of forced labor? Do they read the news on one of your own state-owned websites? Do they engage in discussion about your nation's history by posting to online forums? Most probably all of the above, but in what proportion? How does internet consumption vary between domestic and international usage? Who are the dissidents in your country and where do they live? Who are their friends? Which school did they attend? At this point these questions should be easily answered.

4.1.1 The Dictator's Dilemma

Once you have gathered this data, the key is to develop a control strategy tailored to your particular needs, which fits the specific qualities of your current regime. If you run a more repressive regime (like China or Iran)[69], chances are you will need to allocate more resources to banning or removing content and operating selective "shutdowns". If you run a softer non-democratic state (Russia or Singapore)[69], more energy needs to be poured into propaganda. Often, this even reduces the amount of surveillance needed to monitor citizens, as dissident voices often are drowned in the sea of digital chatter.

Whatever shade of digital control you decide is right for your country, adhere to it and enforce it at all costs. You may be forced to choose between economic benefits and political risk. Having a more liberal approach will boost your economy by developing a service industry and online commerce, but also heighten the risk of your population developing a sense of political autonomy.

In many cases, a combination of many interfering actors will yield the best results. A sophisticated cyber-police that bans selected content swiftly and effectively, a heavy propaganda artillery, a strong political will to enforce legislation and a thriving private industry to produce centralizing tools that facilitate surveillance is one possible configuration.

It's important to note that we have certainly not yet exhausted all the possibilities for control over cyberspace (non-democratic regimes constantly innovate on this front) and you are encouraged to experiment with new techniques adapted to your specific needs in order to stay ahead of the curve. The number of options at your disposal is usually proportional to the complexity of these technologies, and the speed at which they emerge and develop in the private industry.

4.1.2 Politicizing versus depoliticizing

The next set of recommendations can unfortunately not be offered as a pre-packaged set of universal rules to follow. They should help a country's leader decide if, and to what extent, citizens will be engaging in political life and under which circumstances. I will touch on the two main options that should be available to you depending on the type of non-democratic regime you are running: authoritarian or totalitarian. To stay consistent with your current policies, dictators of authoritarian states who usually allow independent social and economic institutions (for example in Singapore) might prefer to heavily depoliticize their population, while the more holistic approach of totalitarianism (Stalinist Russia or Nazi Germany for example) would suggest that turning everything into a political act might be a wiser choice. Furthermore, it's important to mention that the totalitarian approach will be harder to execute successfully since it relies on perfect control of users' online activity. It would be advisable if you are in such a situation to consider slowly migrating to the more subtle, mind-numbing depoliticizing of your population.

Politicizing or depoliticizing a large audience takes time. It cannot be achieved overnight. When trying to instill a collective state of mind in a large body of people, there is no quick fix and small incremental steps must be taken to avoid jumping the gun. It's also important to point out that if you start this process when people are in the streets protesting and organizing through social media, you are doomed to fail. If you've arrived at this point, you unfortunately have other problems to solve and should either jump directly to the last part of this guide on damage control and social media tactics, or start over at the beginning. As Ethan Zuckerman, director of the MIT Center for Civic Media wrote in his popular internet piece "The First Twitter Revolution?", "any attempt to credit a massive political shift to a single factor -- technological, economic, or otherwise -- is simply untrue. Tunisians took to the streets due to decades of frustration, not in reaction to a WikiLeaks cable, a denial-of-service attack, or a Facebook update".[15]

When you start the process of (de)politicization, be methodical and build up your political capital slowly. You should see this endeavor as a long-term investment.

Strategy A: Depoliticization means entertainment.

In C.S. Lewis' satirical Screwtape letters, Screwtape, a senior demon working for the Devil, explains to his nephew at the beginning that "the trouble about argument is that it moves the whole struggle onto the Enemy's own ground.[...] By the very act of arguing, you awake the patient's reason; and once it is awake, who can foresee the result?"[16] What Screwtape is essentially suggesting is to stay away from polemic, argument and confrontation. The best way to not awaken someone's mind is to distract it and make sure it stays dull.

You should follow this example as entertainment is probably the best pressure valve to pacify a population living under your guidance. Lewis' book is also a recommended read, as it holds many useful tactics for psychological coercion. To this end, entertainment media can help you achieve your goals. If you run an authoritarian state and tolerate a private sphere within society, talk shows, funny image websites, video websites and blogging platforms can be extremely powerful allies. Even more "dangerous" platforms such as Wikipedia and social media outlets can be tremendous hypnotizers if censored and curated carefully. The only important rule to follow in this context is to block any sensitive content. Render social and political issues non-visible or make them appear trivial. David Letterman's show is okay, discussion forums about your national history are not. Documentaries about wildlife conservation are okay, short films about living conditions in other nations are not. Sports coverage should be encouraged, self-help books may be advertised and gambling can be wildly popular, but freedom of press should not be a topic to be found anywhere on the internet. In practice, this will often translate into banning domestic content in the local languages and opening up to international content in English. Follow the example of Iran which actually censors more Persian-language content than English-language content.[64]

As you filter and inspect your citizen’s internet packets (with the help of the friend you appointed to manage these affairs), disable and crack down on any mention of “hot” topics but make sure to open the gateways to illegal downloading of popular series and TV shows. As you restrict freedoms, it’s important for your population to be able to unwind, laugh a bit and sense a superficial joy. Provide them with gossip material for the next day. There is a balance to be struck between effective suppression and benign entertainment. Without it, you risk feeding a sentiment of desperation, which eventually leads to angry masses. Letting citizens visit social networking sites as is done in China means that benign entertainment occupies time and mental space that might otherwise be used by many young people for critical reflection, which can be dangerous to your regime. Let them flirt on social networks, let them discuss the previous night’s outing, let them post pictures of themselves often, let them send funny video links to each other by email. Give procrastinators the impression that they are free to express themselves as much as they fancy, because there is nothing dangerous about a narcissist, self-absorbed population. They are not the ones likely to trigger a revolution.

Indeed, if you run a more liberal authoritarian regime, letting entertainment media flood your internet can be an effective numbing strategy, not to mention an economical one (its cost is nonexistent if you let others produce the content for you). In their recent study “Opium for the Masses: How Foreign Free Media Can Stabilize Authoritarian Regimes” Kern and Hainmueller demonstrated that “foreign free media actually helped stabilize one of the most oppressive communist regimes in eastern Europe, the German Democratic Republic”. Their discoveries, albeit counterintuitive, are important. Eastern Germans had access to Western television which “offered an escape from bleak socialist reality at least for a couple of hours each day”. In fact, “East Germans who tuned in to West German television became more, and not less, satisfied with the East German regime. Instead of fostering resistance to the communist dictatorship, the narcotizing effect of television served to stabilize rather than to undermine communist rule.”[18] The Russian government has seemingly learned much from these techniques. As Morozov points out: “From the governments’ perspective, it’s far better to keep young Russians away from politics altogether, having them consume funny videos on Russia’s own version of YouTube, RuTube (owned by Gazprom, the country’s state-owned energy behemoth), or on Russia.ru, where they might be exposed to a rare ideological message as well. Many Russians are happy to comply, not least because of the high quality of such online distractions.”[33]

As Screwtape the Demon himself described mortals, “Never having been a human, you don’t realize how enslaved they are to the pressure of the ordinary.”[17]

Strategy B: Politicizing means constant pressure.

Alternatively, you can choose the second option which is to turn every thought and action, including internet ones, into political acts. This approach would typically go hand in hand with any flavor of totalitarianism and suggest a much tighter control of internet activity. Essentially, you must leave no margin for error and compulsively seek and destroy any sign of anti-regime discourse. Use the internet to turn every user into a zealot who will eventually police his or her peers for you. Every piece of information to be found in digital form should relate in some way to the regime's greatness, otherwise filter it out. Make sure to organize and promote nationalist discourse in forums, (micro) blogs, chat relays, news outlets, free and paid movies, podcasts, music, image boards and every other possible application that bolts onto TCP/IP. To avoid having too many people drop out and ignore your internet because they judge it too extreme, publish important information for citizens online, making it hard to avoid (for example, public services schedules, national holiday information, important national speeches, food stamp printouts, etc). In essence, you simply need to transpose the basic rules that govern your regime into digital equivalents. This might sound simpler at first by virtue of your not needing to dream up a new strategy, remember that controlling cyberspace is not the same as controlling physical space. If you've carefully fulfilled the requirements in this guide, your digital crusade should not be too difficult. On the other hand, if you don't adequately control your physical infrastructure and cannot have direct access to users' raw internet data through politicians under your full control, this can prove much perilous than using Strategy A.

The most obvious example of such an implementation would be North Korea's internet policy, which has adhered to such principles so seriously, we actually don't know very much about their mysterious internal internet - which is actually a nation-specific intranet. Speaking on the subject, Jonathan Zittrain said "In such a situation, any information leakage from the outside world could be devastating, and internet access for the citizenry would have to be so controlled as to be useless".[21] To all appearances, North Korea has managed to pull together an air-tight control strategy and adapted it meticulously to its internet space. Sue Lloyd-Roberts, reporting from North Korea and speaking of its regulated cyberspace, observed that "ordinary people here are forbidden access to the internet. The dear Leader has arranged for all that they need to know".[22]

It would be a lie to claim that this approach could be sustainable in the longer term, as small breaches in such a system - which are very hard to avoid in a completely globalized world - could be catastrophic. It's a gamble to be betting on such a high-risk strategy, but it can definitely keep you going for some years while you prepare a transition towards a model resembling Strategy A.

4.2 Creating a panopticon: best practices

4.2.1 Use your sympathizers

Suppose the unlikely scenario in which your government is suffering from popularity issues. Your citizens are slowly growing unhappy and a shift in public opinion can be felt. This discontent then manifests itself online in small outbursts and you come to realize that only a minority still believe in your authority.

If you’ve met the three essential condition of this guide, you can give the impression of control and consensus. Use the minority of fanatics, have them work for you. Assuming you can influence the topology of heavily used domestic websites, set up online forms to denounce traitors. Create awareness campaigns that denounce “suspect” behavior. Set up groups of online militias that patrol internet forums, chat rooms, online spaces and other dark corners of the internet. Give them compensation and encourage these volunteer spies, as they can often reach online spaces that you will never have access to. Be on the lookout for disgruntled members of the opposing parties (if any exist). By conducting these public campaigns and setting up online forms on websites, the internet population knows that it is being watched not only by you, the state, but also by everyone else.

For inspiration, look to Saudi Arabia where “[citizens] themselves can nominate words and websites they would like blocked by the government firewall”.[57]

4.2.2 Make examples of your opponents

In a paper published this year, Pearce and Kendzior demonstrated how “the [Azerbaijani] government has successfully dissuaded frequent internet users from supporting protest and average internet users from using social media for political purposes”.[46] The attitude of the government can be summarized as: “They punish some people and let everyone else watch. To say, ‘This is what can happen to you”.[47] The paper studied social media activism between 2009 and 2011, a period during which they observed that “frequent internet users became significantly less supportive of protests against the government, indicating that the government’s campaign against online activism was successful.”[48] Surprisingly, during those same years, it was noted that Facebook users grew steadily and social media usage was on the rise.

Former Soviet Union states possess an arsenal of tricks you can learn from, but even on the other side of the globe, smart government officials have cooked up clever ways to discourage “illegal” activities by striking fear into their people. The first decade of the new millennium was a massive battleground for legal skirmishes, pitting the music industry (defending copyright owners) against tech companies, service providers and individuals in the US. The latter were often accused of either facilitating or performing the illegal download and sharing of files (usually music or movies). Both sides won major battles and suffered heavy losses along the way, but the outcome of these battles is not of much interest for the purpose of this guide. Rather, it is compelling to look at the tactics used by the RIAA (Record Industry Association of America) to terrorize a population by targeting harmless individuals and taking them to court. By the end of 2008, the RIAA had filed at least 30 000 lawsuits against individuals in the hopes of creating a powerful deterrent to make individuals think twice before sharing copyrighted material.[27] The number might seem large, but considering the number of cases that were dropped or settled outside courts, and compared to the millions of files transferred peer-to-peer using file-sharing sites (torrent indexes, for example), this number actually amounts to a very small fraction. But the goal of the RIAA and other large corporations was not to make money - for example by asking for $80,000 or $2 million, as different courts have ordered Jammie Thomas-Rasset, a women in her thirties making $36,000 per year, to pay out. They knew that going after everyone who had shared at least one copyrighted file was not only unreasonable but simply impossible, so they set out to scare ordinary internet users instead. The strategy did not really work well in large part because the RIAA has not managed to unequivocally prove the defendants guilty and have them pay in full the amounts sought. They eventually turned to ISPs, wanting to "collaborate" with them to block and filter content.[30]

But you can do much better than this. Assuming your country has tightly integrated political and judicial spheres, it should be much easier to make such ridiculous sentences a reality, just as in Azerbaijan. A survey conducted after the RIAA's campaign against individuals showed that over 25% of respondents who ceased downloading music chose to do so for the following reason : "being afraid to get in trouble/heard about the RIAA lawsuits".[30] While this survey was performed on a small sample, it still provides insight into the level of efficiency that even a rather unsuccessful campaign can have. Imagine if the vast majority of those 30 000 lawsuits materialized into a six digit fine plus a few years in prison. It is not hard to imagine that 25% jumping to 50%, 75% or even more. Consider the following: in July 2009, "the Iranian Parliament began debate on a measure to add websites and blogs promoting 'corruption, prostitution and apostasy' to the list of crimes punishable by death."[56] How's that for a good deterrent?

You should draw inspiration from the RIAA, especially given the very low cost of such spectacular crackdowns. Your digital soldiers can probably find 10 000 "internet criminals" guilty of posting hate speech within a day. People in all types of states have been arrested, beaten, detained and sent to jail, and are facing the death penalty (like Hossein Derakhshan in Iran) for crimes such as “insulting security services”, “violating cultural norms” and “insulting Islam”.[63] Sometimes no reason was given at all and some of these criminals will be in prison many years for simple comments posted online.[64]

Make these cases public, make them personal. Deal with them in such a way that every citizen can easily imagine himself in the place of that poor, unlucky person who just got caught for writing a politically ambiguous statement online. Also, make the implications ideological and moralistic, these trials and accusations should have heavy moral overtones and serve as a lesson about good and evil. Shape your citizen’s behavior using sporadic raids like these and your opponents will eventually not be able to tolerate the psychological pressure. If this reduces the amount of political dissidence online by 50%, you have one half the amount of dangerous data to find, ban and filter out. Be overzealous in your enforcement techniques. When used in conjunction with the first practice (co-ops your regime’s biggest fans lend you a hand in unearthing the bad apples), an effective self-policing pattern with inevitably emerge among your internet users.

4.2.3 Damage control tactics

If people manage to stay secure and anonymous, share politically sensitive material online and start demanding change, you might have a serious problem on your hands. This happened in Tunisia, Egypt and Iran recently. Often, the (de)politicizing process will not work as intended, and then another inevitable problem follows: citizens start organizing dissidence using social media, as no real-world equivalent comes even close to its effectiveness. Being in this situation is not ideal, but while you're in it you should take advantage of it. If your opponents are in a hurry and forget certain important details, you can leverage the power and reach of social media to easily track down and conduct surveillance on individuals. You can then step in and choke the movement swiftly if needed. Social media, as you will find out, opens up certain doors that were always closed to you. When your citizens are angrily protesting in the streets and organizing using social media, consider the following:

- As mentioned in the earlier example regarding Azerbaijan, it is not very difficult to curb your activists' enthusiasm by showing them how unforgiving you will be for even small offenses. Make clear that while social media may be tolerated, any form of political dissidence is completely unacceptable.

- Fostering a revolution is one thing, overthrowing a government another, and replacing it with a new government yet another. There are many gradual steps that most revolutions go through, and social media, the dissident's favorite internet tool, will only help in one or two of these steps - namely organizing and mobilizing. Social media as a tool is not very effective at politicizing an audience, nor is it good at putting pressure on politicians or implementing demands for change. It is an effective way to spread information and, at times, to organize into groups (although when a structure is too horizontal, social media are more confusing than helpful). "Technology alone does not cause political change - it did not in Iran's case. But it does provide new capacities and impose new constraints on political actors. New information technologies do not topple dictators; they are used to catch dictators off-guard."[38]

- There is no need to fear social media for two other reasons. The first is that, although you might witness numerous ideological attacks from social media users on your regime, the ones that matter are the ones coming from within your country. Even if millions of tweets are sent from outside your borders by the diaspora, or anti-regime supporters, what difference does it make if your citizens never see them? This puts pressure on your politicians from other countries' leaders, but it is easily handled with traditional political tactics. Focus on what happens within your country, this is where social media activity should be watched closely. Second, social media are a lot of talk, not much action. It appears that Twitter and Facebook are the best places for non-voting narcissist types to hang out, studies have shown.[35][36] It's rather laughable to examine the average Facebook user's "pages, supported causes and groups" and contrast it with the actual ground support or financial support they receive from the user. "Thanks to its granularity, digital activism provides too many easy ways out. Lots of people are rooting for the least painful sacrifice, deciding to donate a penny where they may otherwise donate a dollar."[37]

- If you effectively decide to enter this arena, be prepared. Have a massive, round-the-clock army of digital warriors. You cannot relent for a single moment as spontaneous online gatherings can explode in a matter of minutes. Also, be ready to let go of strategies you may have used in the past. At this point you will need to take chances, and the worst thing you can do is turn to old media solutions to fight problems of a different nature. Speaking of Iran's internet revolution, Howard offers that "in some ways the regime's response was decidedly old media: expelling foreign correspondents, blocking phone lines, preventing the publication of daily newspapers, and accusing enemy governments of spreading misinformation.” [39] Except for the last tactic about blaming (which is less media-related), these strategies have very little effect on new media crises.

4.3.1 A hypothetical course of action

In practice, here are a few things you can do:

- Blame other regimes for trying to create unrest. Simultaneously, use this opportunity to invigorate nationalistic discourse and blame specific companies that you were seeking to ban on your territory anyways.

- Make sure to point out the close relationships between US government agencies and the CEOs of different companies, and their tendency to swap personnel. A ridiculously clear example of this could be Regina Dugan, DARPA’s Director (Defense Advanced Research Projects Agency) taking a job at Google in March 2012. Stress the fact that many social media tools have a clear political vocation. In February 2012, Mark Zuckerberg, the CEO of Facebook published a letter to explain what Facebook stood for, as he intends on making Facebook a public company. His IPO letter reads: “We believe building tools to help people share can bring a more honest and transparent dialog around government that could lead to more direct empowerment of people, more accountability for officials [...]”[40] This overtly shows Facebook’s intentions to step into the political realm and should be denounced as interference in your domestic affairs.

- There’s nothing worse than Facebook and Twitter on the loose. Conversely, there’s nothing better than Facebook and Twitter under your control :

Once they use social media to connect with each other, you have access to the richest intelligence on your opponents. Iran took advantage of this during the protests following the 2009 election, “while this content was flowing, the government closely inspected digital traffic to try and identify social movement leaders.” Later on, it even pulled the plug during 45 minutes in order to initialize its “deep packet inspection system” [54] Often, this information is even public. If such groups and organizations are private, then simply flex your ISP muscle and exercise your influence on the actual providers to access this information (this is why prerequisite #3 is so important). The gains to be made here are exceptional - including, but not limited to:

- Your opposition’s leaders’ names and contact information
- The internal structures of activist groups
- The connections to other opponents and enemies of the regime
- Information regarding both monetary and intelligence resources
- Private information including pictures, address, phone numbers, emails, etc.
- Insights into their personalities and profiles (where do they shop, what do they eat, etc.)

Obviously, by cross-referencing this data you can draw a very accurate picture of your opponent and easily predict its next move. You can also use this data to arrest, intimidate and destroy your opponent. Put your engineers to good account and extract the immense value out of this raw data, provided by the same services you will be blaming for trying to create unrest and interfering in your domestic affairs.

You have a vast array of tools at your disposal: download face recognition software, which is available free online, and then personalize it to suit your needs. Reverse image search engines will enable you to find the source of certain images. There are even cloud-based WPA-password cracking services (often the standard for home routers) such as CloudCraker[41], if you need to get into people's private home networks. These tools are often free or very cheap but whenever possible you should create your own or subsidize private industry to create them for you.

Exploit the power of third-party applications to gather as much data as you can about your population. Create third-party applications that asks users to connect with their social media account (this is very common) and authorize access to its data. For example, the 2012 Barack Obama Campaign website allows users to sign in using Facebook, which gives access to "name, profile picture, gender, networks, user ID, list of friends, and any other information you've made public"[42] - a real gold mine. Not to mention that these permissions are minimal, and most users wouldn't complain if more were asked from them. The responsibility appears to lie with Facebook to protect users' data, but it is not. Once a user grants access to an application, any the third party can easily scrape and store everything falling under those permissions' parameters. Perhaps the most valuable asset here is the list of friends, which you should pay special attention to when you are tracking down dissidents. There seems to be no record of this being done before, but any smart dictator under pressure from a social media tsunami should build the most effective organizing mobile application for dissidents to use, and force the sign-in process to go through social media. Everything you ever wanted to know about every person that represents a threat to your regime, at your fingertips.

- If you've followed the previous steps, you should have more data about dissidents available to you than needed to disable and arrest the important actors of a movement. Remember, tweets don't make a revolution, people do.

As Appelbaum mentioned when talking about the use of mobile phones to organize protest movements, "[In Iran], they give you enough rope to hang yourself from".[43]

Make sure you do the same.

5. References

[0] The University Of North Carolina. Commentary and Analysis. Retrieved from http://www.unc.edu/depts/diplomat/archives_roll/2004_01-03/palmer_axis/palmer_axis.html

[1] TED. Rebecca MacKinnon: Let's take back the Internet!. Retrieved from http://www.ted.com/talks/rebecca_mackinnon_let_s_take_back_the_internet.html

[2] Washington Post. In Face of Rural Unrest, China Rolls Out Reforms. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2006/01/27/AR2006012701588.html

[5] The New York Times. The Internet Black Hole That Is North Korea. Retrieved from http://www.nytimes.com/2006/10/23/technology/23link.html

[6] BBC News. Life inside the North Korean bubble. Retrieved from http://news.bbc.co.uk/2/hi/programmes/newsnight/8701959.stm

[8] Sectheory. Clickjacking. Retrieved from http://www.sectheory.com/clickjacking.htm

[9] Lessig, L. (2006). Code V2. New York: Basic Books. p57.

[10] By using Facebook's ad creation platform (https://www.facebook.com/advertising/), it is possible to estimate the number of users in a geographical area.

[11] Jacobs, K. (2012). People's Pornography: Sex and Surveillance on the Chinese Internet. Chicago: The University Of Chicago Press. p.28.

[12] ChirpStory. Collection of Tweets from @ioerror. Retrieved from http://chirpstory.com/li/526.

[13] Tor Project. Retrieved from http://www.torproject.org

[14] Morozov, E. (2011). The Net Delusion. New York, Public Affairs. p34.

[15] Foreign Policy. The First Twitter Revolution? Retrieved from http://www.foreignpolicy.com/articles/2011/01/14/the_first_twitter_revolution?page=0,1

[16] Lewis, C.S. (2009). The Screwtape Letters: Letters from a Senior to a Junior Devil. HarperCollins Publishers. Letter 1.

[17] Lewis, C.S. (2009). The Screwtape Letters: Letters from a Senior to a Junior Devil. HarperCollins Publishers. Letter 1.

[18] Kern, H & Hainmueller, J. (2009). Opium for the Masses: How Foreign Media Can Stabilize Authoritarian Regimes. Political Analysis, Vol. 17, No. 4. Chapter 1. p2.

[19] Reuters. China's effort to muzzle news of train crash sparks outcry. Retrieved from http://www.reuters.com/article/2011/07/25/us-china-train-censorship-idUSTRE76O1IG20110725

[20] Morozov, E. (2011). The Net Delusion. New York, Public Affairs. p137.

[21] The New York Times. The Internet Black Hole That Is North Korea. Retrieved from http://www.nytimes.com/2006/10/23/technology/23link.html

[22] BBC News. Life inside the North Korean bubble. Retrieved from http://news.bbc.co.uk/2/hi/programmes/newsnight/8701959.stm

[23] Tor Project. Tor Metrics Portal: Users. Retrieved from https://metrics.torproject.org/users.html

[24] Tor Project. "One cell is enough to break Tor's anonymity". Retrieved from https://blog.torproject.org/blog/one-cell-enough

[25] Tor Project. Iran partially blocks encrypted network traffic. Retrieved from https://blog.torproject.org/blog/iran-partially-blocks-encrypted-network-traffic

[26] Thoughtcrime. sslstrip. Retrieved from http://www.thoughtcrime.org/software/sslstrip/index.html

[27] Overbeck, W & Belmas, G. (2012). Major Principles of Media Law, Boston: Cengage Learning. p277

[28] Overbeck, W & Belmas, G. (2012). Major Principles of Media Law, Boston: Cengage Learning. p278

[29] Overbeck, W & Belmas, G. (2012). Major Principles of Media Law, Boston: Cengage Learning. p279

[30] Jaishankar, K. (2011). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. Boca Raton: CRC Press. p169.

[31] Chaos Computer Club. Chaos Computer Club analyzes government malware. Retrieved from http://ccc.de/en/updates/2011/staatstrojaner

[32] Morozov, E. (2011). The Net Delusion. New York, Public Affairs. p58.

[34] BBC. LiveJournal: Russia's unlikely internet giant. http://www.bbc.co.uk/news/magazine-17177053

[35] Mashable. STUDY: Social Media Is for Narcissists. http://mashable.com/2009/08/25/gen-y-social-media-study/

[36] http://www.eurekalert.org/pub_releases/2011-08/apa-sng072711.php

[37] Morozov, E. (2011). The Net Delusion. New York, Public Affairs. p190.

[39] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.8

[40] Techcrunch. Facebook's S-1 Letter From Zuckerberg Urges Understanding Before Investment. Retrieved from http://techcrunch.com/2012/02/01/facebook-ipo-letter/

[41] CouldCracker. Retrieved from https://www.wpacracker.com/

[42] The Guardian. Obama, Facebook and the power of friendship: the 2012 data election. Retrieved from http://www.guardian.co.uk/world/2012/feb/17/obama-digital-data-machine-facebook-election?INTCMP=SRCH

[43] The Bureau Of Investigative Journalism. In Video – Jacob Appelbaum on phone tracking. Retrieved from http://www.thebureauinvestigates.com/2011/12/21/in-video-jacob-appelbaum-on-phone-tracking/

[44] The New York Times. Pakistan Builds Web Wall Out in the Open. Retrieved from http://www.nytimes.com/2012/03/03/technology/pakistan-builds-web-wall-out-in-the-open.html

[45] Packard, A. (2010). Digital Media Law. Malaysia : Blackwell Publishing. p.26

[46] Pearce1 K. E. & Kendzior S. (2012). Networked Authoritarianism and Social Media in Azerbaijan. Journal of Communications. Vol 62. Issue 2.

[47] Pearce1 K. E. & Kendzior S. (2012). Networked Authoritarianism and Social Media in Azerbaijan. Journal of Communications. Vol 62. Issue 2.

[48] Pearce1 K. E. & Kendzior S. (2012). Networked Authoritarianism and Social Media in Azerbaijan. Journal of Communications. Vol 62. Issue 2.

[49] Baloyra E. A. & Morris, J. A. (1993). Conflict and change in Cuba, University Of New Mexico Press. p182

[50] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.11

[51] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.4

[53] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.6

[54] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.6

[55] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.8

[56] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.10

[57] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.44

[58] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.44

[59] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.212 (Appendix A)

[60] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.57

[61] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.80

[62] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.80

[63] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.114

[64] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.115

[65] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.119

[66] Lessig, L. (2006). Code V2. New York: Basic Books. p61.

[67] Lessig, L. (2006). Code V2. New York: Basic Books. p73.

[68] Morozov, E. (2011). The Net Delusion. New York, Public Affairs. p57.

[69] The Economist. The Democracy Index 2011: Democracy under stress. Taken from https://www.eiu.com/public/topical_report.aspx?campaignid=DemocracyIndex2011 (China rated 141st, Iran 159th, Singapore 81st and Russia 117th)

6. Notes

1. We know that M.Xyz has an IP address (an internet address for every computer connecting to the network) of 111.111.1.1 for a given time, since the ISP has dispatched this address to him. One can subsequently look at what internet resources address 111.111.1.1 is requesting and understand what M.Xyz is up to. For more details see [66]

2. This could be compared to owning and controlling a highway, but not the access and exit ramps. The data flowing within the network is hard to reach, but the way it enters and exits the network is left up to the user.

3. For an entry point, exploit the laziness of users when they use faster, less secure applications in combination with your control of IPS' to reveal requesters' data. For the exit point, make sure to control many Tor exit nodes and diligently record all data

4. Certain users were not able to connect to the Tor network directly, so "bridges" were developed. Dictators understood how to block Tor traffic based on its type, so "Obfsproxy" was created to make it appear to be something else.

5. As Moxie Marlinspike demonstrated with his tool SSLSTRIP during the Black Hat DC 2009 Hacker conference, you can act as a "man-in-the-middle" to intercept HTTP requests containing HTTPS links in the response, fooling many users (in the small test he ran, 100% of them) into thinking they are using a secure connection.[26]

7. Note from the author

I believe in democracy as a potent vehicle for equality, transparency and security around the world. There should be more democratic countries and all of us should live in a state which safeguards these values. I completely agree with Mark Palmer, who worked in Eastern Europe as a US ambassador during the last years of communism in the 1990s when he says “I think the goal should be universal democracy by the year 2025”[0]. I wouldn’t mind it happening in 2020 or 2015 either, but I know it’s not likely to materialize.

At the time of writing, a wave of unprecedented optimism about the undisputed role played by technology in overthrowing non-democratic regimes is sweeping the Western world. In my short years as a digital native, I can’t recall a period of time when myths about digital technology were more bloated and extravagant than now. There is a dangerous idea circulating in Western discourse that the internet has a natural inclination to produce a specific brand of Western democracy and sprinkle freedom from the tip of its fiber-optic wand. If we are to fulfill Palmer’s goal, we need to think critically of claims such as “if you want to liberate a society, just give them the internet” by internet activist Wael Ghonim.[1]. These assertions are simplistic and often dangerous. We need a more nuanced approach than what Western media proposes if we are to solve authoritarian states - and more of our imagination too. I’m hoping this essay will help with the latter, which can hopefully lead to the former.

I’d like to add my voice to the current choir of states demanding more democracy, more freedom and more accountability in places like Iran, China, Syria and North Korea. But our internet strategy and foreign policies regarding these states frequently encourage these regimes' totalitarian ways. We don't know that much yet about how dictatorships use technology to alienate their citizens in many countries. On the other hand, we know much more than we like to believe about technologies we hope will overthrow despotic leaders by virtue of their mere presence. We should focus on that knowledge and make decisions based on that knowledge, rather than on projections of our own ideals onto the technology itself. We need to turn the tables around and wonder, if only for a brief moment, how we might be hurting democracy's case by considering the internet as an end rather than a means.

Finally, I'd like to stress that I am not an expert on international affairs, foreign policy or even politics. I have written this essay as a technologist and fine arts student with software engineering experience and a mere interest in the humanities.