future internet

MDPI

Article

A Survey of Defensive Measures for Digital Persecution in the Global South

Louis Edward Papa [1,2] and Thaier Hayajneh [2,*]

[1] Graduate School of Arts and Science, Fordham University, New York, NY 10023, USA; papa@fordham.edu
[2] Fordham Center for Cybersecurity, Fordham University, New York, NY 10023, USA
* Correspondence: thayajneh@fordham.edu

Received: 27 July 2020; Accepted: 25 September 2020; Published: 29 September 2020

Abstract: This paper examines the phenomenon of digital persecution in the Global South and evaluates tools that defend against it. First, the paper explains the nature of persecution and its digital incarnation. It then provides a contextual overview of real-world instances of digital persecution in seven Global South countries. The possible defensive technologies against censorship and surveillance are discussed. The article goes on to discuss barriers to technology adoption in the Global South, explains the security implication of these difficulties, and examines the role that human computer interaction (HCI) metrics could play in overcoming these challenges. Finally, the paper surveys the viability of sixteen security tools in a Global South context. The survey results were mixed, with 37.5% of the reviewed tools being deemed to be inviable for use in the Global South to defend against persecution. Prescriptive recommendations are provided for creating security tools that are universal, simple, and effective.

Keywords: persecution; oppression; free software; global south; cybersecurity; HCI; human rights

1. Introduction

In a few short years, most internet users will be the poor of the Global South. Internet technology is often presented as a panacea for the common troubles in developing economies. Internet technology can assist in solving the problems of disease, lack of clean drinking water, limited social mobility, etc. However, many of these four-billion people live in persecuting societies, with nominal education and income levels. Payal Arora explores some of the unique challenges to these users in his study The Bottom of the Data Pyramid: Big Data and the Global South [1]. These netizens lack the social, political, and economic power to challenge how their data are collected and used. Despite the technology giants' utopian prophecies, the sobering reality is that the internet will likely be used to oppress most of the world.

A seemingly never-ending deluge of major stories involving government surveillance and censorship has swamped the Western media. This has created an environment of distrust and paranoia among the citizenry, who are increasingly turning towards defensive technologies that thwart this activity. The vast bulk of discussions on internet surveillance and censorship are based in the Global North, where most netizens enjoy a wide range of legal protections and are not beholden to strict social mores. This is the natural result of several high-profile instances that reveal the ethically questionable online activity of intelligence and law enforcement agencies in the West. See Citizens under Suspicion: Response Research with Community under Surveillance by Arshad Imitaz Ali [2].

However, successfully implementing defensive technologies usually demands some sophistication; many products require users to be savvy, and some are expensive. Global North internet users benefit from a relatively high standard of living and have already experienced several iterations of any given technology. Conversely, people of the Global South are often lacking in

opportunity and access to education. Therefore, digital persecution presents a greater risk to them than almost anyone in the Global North.

This article uses the term "Global South", which is often used interchangeably with "developing countries". This terminology is frequently subject to debate. For this article's purposes, Global South refers to the countries or regions listed as developing in the United Nations publication "Standard Country or Area Codes for Statistical Use," commonly referred to as the M49 standard [3]. China, Egypt, India, Iran, Mexico, North Korea, and Pakistan are all considered to be the Global South by this standard. The term is for convenience only and it is not intended to criticize or impugn a country's development stage or process.

The unique dangers this resource gap poses to underprivileged populations is discussed in greater detail in Nir Kshetri's article Big data's impact on privacy, security, and consumer welfare [4]. Technology evangelists myopically present a rosy image of the future where greater connectivity invariably has positive consequences. This is self-evidently unrealistic in a world where most people are in no position to dictate the terms of those connections. There is also an issue of inherent biases being built into an application. If the author of an algorithm has a bias, it will be reflected in the output of that algorithm (ehich raises an interesting question: Could an artificial intelligence be racist if its developer had unconscious biases? Conversely, could an artificial intelligence prevent that from happening?). This can have a negative impact on marginalized communities who are already affected by stereotyping.

Meanwhile, relatively few studies have been done on digital persecution in the Global South. Some worthwhile articles on the subject include work by Amnesty International [5] and Privacy International [6]. What little research exists rarely investigates the technical details. There are dozens and dozens of articles discussing the U.S. National Security Agency's snooping program and the technical capabilities of the tools that they implement. However, when it comes to Pakistan, a nuclear armed state with the seventh largest population in the world, Zubair Nabi's The Anatomy of Web Censorship in Pakistan is probably one of the only technical articles on the subject available in English [7].

The primary methods of persecution that this study focuses on are surveillance and censorship. Global South internet users need effective security tools. To that end, this article evaluates widely available defensive technologies in the context of the Global South. It provides an actionable assessment of existing defenses for people with low-education and living in poverty-stricken areas under oppressive regimes. A defense's effectiveness is determined by how well it counters surveillance or censorship and how easily an average person in the Global South could implement it. Most tools are technically effective, but ease of use is a major impediment to adoption. It was expected that most tools will prove inviable, but this study had mixed results. Prescriptive recommendations on how to make existing tools more available to marginalized communities is provided. The main contributions of this paper are as follows:

- Provides crucial context for understanding the nature of digital persecution and the severity of that threat to people in the Global South.
- Provides a practical overview of digital persecution as it is practiced in China, Egypt, India, Iran, Mexico, North Korea, and Pakistan.
- Discusses various types of security tools and their role in defeating digital persecution.
- Examines issues preventing technology adoption in the Global South, such as the lack of education, infrastructure, and trained technology professionals.
- Examines standards for measuring security tool viability, and illustrates which metrics are most important to consider in a Global South context.
- Proposes methodologies for reviewing security tools for use by marginalized and poor netizens, where external factors greatly impact the user's ability to effectively implement a given defense.
- Performs a survey of sixteen security tools and evaluates their viability for use by people in the Global South.

For this study, factors, such as ease of use and simplicity, are the basis of determining a tool's viability. There has been a substantial amount of research on evaluating human computer interaction (HCI), technology adoption, task difficulty, and usability. The common-sense thesis behind all of this previous research is that the more difficult it is to use a tool, the less likely it is that a human will use it correctly [8]. Obviously, this undermines the purpose of the tool, especially in a security context. After all, if a user incorrectly implements a security measure, then he could erroneously believe that he is safe when he is not and put himself at greater risk.

The lack of studies on the viability of security tools in the Global South highlights the necessity of this research. It is surprising that material on this subject is so hard to find, given the sheer size of the population that digital persecution could affect. The most likely explanation for this gap is a lack of economic incentive. Over half of the Global South makes less than $2.00 a day [9]. While many of these low-earners are not typically netizens, the current trend of internet penetration would imply that they soon will be.

The structure of this paper is as follows: Section 2 describes the nature of digital persecution and this paper's focus on censorship and surveillance. Section 3 illustrates how digital persecution is conducted in seven Global South countries. Section 4 explores how various technologies could be used to thwart censorship and surveillance in these countries. Section 5 discusses the metrics for evaluating a tool's viability and justifies which are appropriate in this context. Section 6 describes the methodology of testing, which tools were tested, and why. Section 7 is a discussion on the test results and it includes tables showing the results. This section also explores open issues and avenues of future study. Section 8 concludes the paper.

2. The Nature of Persecution and the Meaning of Digital Persecution

The state can be understood as a "monopoly of legitimate violence". The state sanctions citizens to act collectively where individual action would be considered immoral, indecent, or illegitimate. Only the state can declare war, enforce laws, punish criminals, collect taxes, and so on. Persecution is "deliberate and socially sanctioned violence. . . directed through established governmental, judicial, and social institutions, against groups of people defined by general characteristics such as race, religion, or way of life" [10]. It is legitimized aggression against people over arbitrary or accidental characteristics.

The common thread among persecuting societies is an orthodox/heretic dialectic. A society is orthodox when its members are expected to adhere to an overarching belief or attitude. Therefore, anyone who does not fit into this orthodoxy is a heretic. The orthodox perceive the heretics as a "pollution" or threat that must be purged. The purge takes on many forms: extortion, imprisonment, enslavement, humiliation, exile, murder, etc. All of this violence is socially permissible, and the reasons that a person would be targeted are often inseparable from the person. This means there is no legal recourse and no escape, and therein lies the severity of the threat. If an individual faces execution because of his race, he cannot change his race to avoid this fate, nor can he seek help from the state because the state sanctions his murder.

Digital persecution is merely computer facilitated persecution. Information technology (IT) enables state actors to reach millions of people at once, so the threat increases exponentially. It also makes persecution exceedingly easy. In the past, inquisitors would have to threaten and torture people to get information out of them. Secret police would have to follow people, tap their phones, and intercept their letters. Today, with modern social networking, there is no need to torture anyone, because everyone is already voluntarily informing on everyone else. Sending the secret police out to track people is unnecessary when anyone with a smartphone is potentially carrying a surveillance device around with him in his pocket. Prof. Eben Moglen lectured on this subject at the re:publica 2012 conference in Berlin [11].

2.1. Surveillance

There are two kinds of surveillance: targeted and mass. Targeted surveillance involves tracking a specific person with the goal of discovering specific information. Planting spyware on someone's computer would be an example. Mass surveillance involves monitoring large groups of people without specific attention being paid to any one person. An example would be collecting an entire town's phone records in order to go through them later. The distinctions between targeted and mass surveillance are explored further in *Crypto and empire: the contradictions of counter-surveillance advocacy* by Gurses, Kundnani, and Hoboken [12].

Surveillance accomplishes several important goals for the state. First, it aids in the discovery of criminal activity. While this may be justifiable in many cases, keep in mind that criminal justice is arbitrarily enforced in a persecuting society. Second, surveillance provides the state with information about popular trends and attitudes. Third, there is a panoptic effect, and this is likely the intended effect of mass surveillance. People in persecuting societies rarely know when they are being watched, so they must assume that they are being watched all the time. People will behave differently if they believe that they are being monitored. They are more careful in their word choice and activity. This becomes a passive method of enforcing orthodoxy, and secret police will often behave conspicuously for this exact reason. Martin Sokefeld and Sabine Strasser discuss the experiences of anthropologists dealing with this exact problem while engaging in fieldwork: "Surveillance has strong disciplining effects on fieldworkers, because, knowing that we are watched, we become very careful about where we go, whom we meet, which topics we address and what to ask" [13].

The exact methods and legal rationales for surveillance will vary from country to country. However, state monitoring of social networks, such as Facebook and Twitter, may prove to be the greatest source of risk in the future for the Global South. Aside from the obvious sharing of information that goes on, a user's unconscious behavior on social media can reveal data that he would not normally share. For example, a user could unwittingly telegraph their sexual orientation or religious beliefs. The risk becomes clear when one considers that there are several Global South countries where being a homosexual and/or an atheist is a crime punishable by death.

2.2. Censorship

There are two forms of censorship: erasure and suppression. Erasure involves destroying any media deemed indecent, immoral, subversive, or heretical. The digital incarnation of this includes deleting media and taking down websites. Suppression involves regulating, blocking, or shutting down the means of distributing prohibited media. Blocking websites, punishing users who visit those websites, coercing bloggers, or even shutting down internet access are all examples of digital suppression.

Internet censorship varies in its scope and depth from country to country. Approximately 25% of the world's population live in states where internet censorship is extreme. Governments will enforce censorship for the stated purpose of "protecting public morality. . . national security, and social stability" [14]. However, there is rarely any consistency in how censorship is enforced. Often, it is merely a means for silencing political dissent or oppressing a minority. Censorship also serves the purpose of clearing space to be filled with propaganda. When all other points of view have been quashed, only the orthodoxy remains.

3. The Scope: Examples of Digital Persecution in the Global South

It is important to understand the reality and scale of digital persecution. This section examines digital persecution in seven Global South countries: China, Egypt, India, Iran, Mexico, North Korea, and Pakistan. This provides a real-world understanding of how digital persecution is practiced. Similarities between different countries will become clear.

The below review is not intended to be extensive, but to highlight the scope and nature of the threat. The seven countries reviewed represent a combined population of over 3.1 billion people, about 75% of the Global South [15]. Access to the internet is highly regulated and throttled. Online content is regularly censored, sometimes at the internet service provider (ISP) level, and large swaths of the internet are occasionally shut down. Their governments utilize advanced means of mass surveillance, but they also target individual civilians with spyware. Government agents monitor social media, and users are imprisoned and executed for posting subversive content. If this continues and becomes the norm, then the future internet will be a tool of persecution for most of the world.

3.1. China

China has the world's largest population of internet users, with over 293 million by 2009. Technology proponents assumed that greater internet penetration in China would inevitably lead to greater democratization, but this has not materialized. On the contrary, the Chinese government views virtually all internet technology as a potential tool for control [16]. Several technology corporations have participated (perhaps unintentionally) in the creation of a massive censorship and surveillance network [17]. The Golden Shield Project, which is known colloquially as the Great Firewall, blocks huge segments of the internet that the Chinese government deems to be inappropriate or subversive. Briefly, the system eavesdrops on traffic between China and the outside world. When a request is made for a prohibited site, Golden Shield injects fake TCP reset packets that cause the sender and receiver to stop communicating with each other [18]. When the Golden Shield Project was originally completed in 2006, the system consisted of over 800,000 computers, 60 application systems, and eight databanks. It has likely grown since then [19].

Along with Golden Shield, there are tens of thousands of human government agents monitoring Chinese social media. Users who post subversive content may face imprisonment [20]. The threat of facing any legal prosecution in China is enough reason to self-censor. Unfair trials and wrongful convictions are common. It is estimated that China executes more people than any country on Earth. However, it is impossible to say exactly how many people are executed each year, as the Chinese consider the number to be a state secret. The death penalty is implemented for both violent and non-violent crimes [21].

3.2. Egypt

Significant political turmoil has rocked Egypt since the January 25 Revolution of 2011, which ended the 30-year reign of President Hosni Mubarak. Leading up to 2011, the Mubarak government was widely characterized as corrupt. The Mubarak government aided the growth of internet in Egypt for economic reasons. However, Mubarak imposed severe restrictions on media through "emergency powers" that had been in place since the rule of the previous president, Anwar Sadat. While internet technology (specifically Facebook) is often credited for the empowerment of the Egyptian people, the government has used the internet to monitor, track, harass, and eventually jail political dissidents. The filtering of internet sites was generally not done. However, secret police surveille the citizens while using the internet [22].

3.3. India

Network Traffic Analysis (NETRA) is the Indian internet surveillance system. A 2016 case study of this system explains that it is used to target people and groups "that have a history or an inclination to carry out heinous and opprobrious acts" [23]. It filters internet traffic looking for words, such as "attack", "kill", "bomb", etc. It then reports the usages of the word and the associated IP address. NETRA monitors communication done via email, Google Talk, Facebook, Skype, Blackberry, instant messages, as well as blogs and forums. It can even analyze some encrypted traffic. However, the system is unable to discern the meaning or context of a word and it must rely on pre-defined filters. This means that an individual could erroneously become an object of suspicion.

3.4. Iran

Iran's government controls the internet through the Telecommunication Company of Iran, a state-owned monopoly. All ISPs are linked to this company and they must adhere to its standards. This means censorship can take place at the ISP level. Aside from blocking millions of websites, the government also suppresses communication by throttling connection speeds to 128 Kbps [14]. The regime has also imprisoned netizens for expressing objectionable views online. During the "Green Revolution" of 2009, the regime blocked access to Facebook, YouTube, and other sites. Secret police infiltrated social media sites to surveille and intimidate political dissidents [22].

One of the stranger responses to the Green Revolution is the government's effort to create a "halal internet". Rather than relying on a complicated filtering system, like China's Golden Shield Project, the Iranian government is pursuing a national intranet that will not connect to foreign sites. Iranians would only be able to connect to sites that are based in Iran. This would empower the regime to further isolate Iranian netizens from the rest of the web [24].

3.5. Mexico

A 2017 New York Times article entitled *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families* describes how the Mexican government purchased a spyware program, called Pegasus, to target their own citizenry [25]. Pegasus, created by the NSO group, was sold to Mexico's federal agencies on the condition that it only be used for investigating terrorists and drug cartels. However, Pegasus has been targeted against journalists, academics, and human rights lawyers, as well as their families. Briefly, the Pegasus spyware is installed on a smartphone when a user clicks on a malicious link in a text message. The message is made to pique the interest of the recipient, such as claiming that the link contains a photo of armed men outside the recipient's house. Clicking the link installs the spyware and leads to a page that appears broken. Once installed, Pegasus monitors texts, emails, calls, calendars, and contacts. It can clandestinely turn on the microphone and camera, effectively turning the phone into a surveillance device. While the Mexican government's involvement has not been confirmed yet, the circumstantial evidence is significant. For one, the NSO Group asserts that only a government agency can use the spyware. Furthermore, all of the targeted non-criminals are people critical of the government. This includes lawyers investigating the unsolved disappearance of 43 students that were abducted by Mexican police.

3.6. North Korea

North Korea was almost not included here, because internet users are an extremely rare class in this country. Often referred to as the Hermit Kingdom, North Korea is the most severely censored country in the world [14]. People in North Korea have virtually no knowledge of the outside world and are rarely allowed to speak to foreigners. At the One Young World Summit in 2014, Defector Yeonmi Park described her experience living in North Korea: watching a Hollywood movie, or making an international phone call without government approval, could merit a death sentence. There is only one channel on television. Dissent against the regime could result in three generations of a family being imprisoned [26]. Internet access is tightly limited to people within the government and high-level members of the ruling party. The purpose of this intense restriction on information is to protect the power and prestige of the Kim family's dictatorship [27].

3.7. Pakistan

Pakistan is a large, Islamic traditionalist country that has struggled with internet adoption. A 2013 publication by Jahanzaib Haque describes issues surrounding internet adoption, surveillance, and censorship in Pakistan [28]. There is a significant gap between urban and rural internet access, with rural netizens representing only 3% of Pakistan's internet users. Many users still rely on dial-up and mobile phone connectivity. The Pakistani government's heavy-handed approach to internet regulation,

Haque argues, is one reason for this hampered development. The Pakistani Telecommunication Authority (PTA) oversees most og the matters involving the internet, including regulation, licensing, and censorship.

The Pakistan government employs sweeping powers to surveille citizens while using internet technology. Most of Pakistan's internet traffic is routed through a single backbone, called the Pakistan Internet Exchange (PIE). This makes monitoring a simpler task as most user traffic is funneled through a single point. The use of virtual private networks (VPN) and encryption are illegal, and ISPs are required in order to retain records of traffic for 90 days, further simplifying the state's surveillance efforts. At least one command and control (C&C) server for FinFisher spyware has been found on the government's network. This is proprietary spyware that takes advantage of common unpatched vulnerabilities.

The PTA is incredibly censorious, and it will block entire websites hosting content deemed as offensive, even if the content is only hosted on one part of the site. It has been estimated that the PTA blocks anywhere between 20,000 and 40,000 websites, but the true number is probably much higher. In 2012, the PTA sought to purchase filtering software from Netsweeper, a Canadian firm, which can categorize 10 million new websites each day. Blocking can be done at the ISP level, and ISPs that fail to comply with the PTA's blocking requests risk losing their license. Further, the censorship decision-making process is not transparent and website blocking appears arbitrary.

At least three different blocking methods are used: first is DNS level blocking, wherein the users are given the impression that a requested page does not exist. Second is HTTP level blocking, where users are redirected to a warning page. Third is forged HTTP response injection, wherein the user receives a packet with an injected warning message, and the connection with the blocked site times out [7].

4. Exploring Defensive Measures against Digital Persecution

Living in a persecuting society where internet technology is used to surveille and censor the citizens can be perilous for the disenfranchised. However, netizens in these countries are adaptable and implement their own tools and strategies for defeating state internet controls. Some methods are simple behavioral strategies. For example, internet users in China [29] and South Africa [30] will use homonyms or thinly veiled language to get around censorious filters. Others rely on defense technologies, which are the focus of this article. A defensive technology can be useful against surveillance, censorship, or both.

Proxy sites can be used to get around site blocking, like what is found in Pakistan. These are publicly accessible webpages that perform queries on behalf of their visitors. For example, if YouTube is blocked in a country, then a user can visit the proxy site instead and request the content they want through there. The traffic is not blocked, because it is not detected. This can also thwart mass surveillance, because, from the ISP level, it appears that the user is only sending traffic and receiving traffic from the proxy site.

An improvement over proxy is VPN. VPN services provide an encrypted connection between two points over the public internet. These can allow users to hide their internet traffic from state monitors operating at the ISP level. VPN can also allow a user to get around site blocking. These are not the same as onion networks, like Tor. Volunteers run the nodes in an onion network where a VPN's nodes are privately owned and managed. This can confound state efforts at seizing the traffic, as there is no single corporate entity who can hand over logs or user data. However, malicious actors may control the nodes in an onion network, so there are still risks.

Mainstream social media sites, like Facebook and Twitter, have shown a willingness to cooperate with persecuting governments. In response, privacy-conscious netizens have turned to alternative social media. These sites that have a rebellious culture, value anonymity, celebrate breaking from social norms, and will actively defy attempts to censor them. However, government agents can still operate on these sites like any user.

These tools work well against mass surveillance and censorship. However, a user seeking defense against targeted surveillance tactics, like Pegasus in Mexico, will have to consider endpoint protection. This includes antivirus software, which can thwart state-sponsored malicious code. Malware developers will try to create viruses that evade antivirus detection, so this will not always be effective.

Encryption on local storage will also thwart targeted surveillance. Provided that the user does not share or improperly store the keys, locally encrypted files will be unreadable if a computer is lost or stolen. This protects the user from the efforts of secret police, who may confiscate electronic equipment. A user can also destroy local files using wiping technology. These are tools that overwrite data on the disk with known values, which makes it impossible to recover them. Wiping data would be important to a user concerned that files on his computer may be used as evidence against him.

Finally, there are security-centric OS. In many cases, security is an afterthought in designing and OS. Indeed, there have been instances where an OS was deliberately made insecure and backdoors are left for developers or law enforcement. A security-centric OS is a system where the user's privacy, anonymity, and safety are prioritized over performance. These systems may use onion networks as a default or destroy evidence after every restart.

An end user ought to employ more than one of these security tools in order to achieve the strongest defensive posture. An example of an ideal scenario: Johann, who lives in a persecuting society, communicates with his friends on an alternative social network that he connects to via a VPN. He has antivirus running on a computer with a security-centric OS. When creating sensitive files on his computer, he encrypts them, and he uses wiping software that overwrites the data when he destroys them.

In this example, if the state monitors Johann's ISP, his identity remains protected because he uses VPN, which encrypts his traffic. If his computer is confiscated, then the files on it are either encrypted or wiped, and cannot be recovered by the secret police.

Using these tools can be a risk to the user in some circumstances. The mere appearance of trying to evade persecution can invite greater scrutiny. In several of these countries, like Pakistan, the use of a VPN is itself illegal and will carry a penalty. The risks of using these tools must be weighed against the risks of not using them, and this is going to vary greatly from region-to-region and person-to-person. Ultimately, it is a decision that every individual must make for himself.

Further, the tool can pose a risk to the user if the user does not use it correctly, or if the user does not adequately understand what the tool does. A user who incorrectly implements a defensive technology will likely put themselves at even greater risk than someone not using one at all. A security tool that is not made to serve a Global South audience will provide the least amount of protection to the users who are most at risk.

5. Metrics for Consideration

5.1. Security Technology and the Global South Context

Many security tools are developed anticipating that their users have some amount of savviness, are sufficiently educated, or have access to adequate resources. This is decidedly not the case for many people in the Global South where widespread technology adoption faces many challenges. First, there is a often a lack of requisite education, and UNESCO notes there is a significant gap in schooling between the Global North (where these tools are usually made) and many Global South nations [31]. Second, governments in the Global South rarely make investments in IT. When they do, they often rely on the assistance of Global North nations who do not sufficiently understand the countries they are helping. Thus, their assistance is flawed, and their aid is made ineffective. Third, most Global South countries lack telecommunication infrastructure. There may only be a few telephone lines or limited power supply. Internet cafes are the sole source of internet for many, and those tend to be only found in urban areas. Fourth, well-trained technology professionals are uncommon in these areas. It is very

difficult to create and maintain IT infrastructure without skilled IT personnel. Despite these challenges, the growth of internet penetration in the Global South is simply staggering. For example, internet penetration in Africa grew over 3606% between 2000–2012. That is a rate of growth six times larger than North America and Europe combined. Still, only a fraction of Africans have internet access [32,33].

Case studies in Saudi Arabia [8] and Ghana [32] highlight common issues that surround user adoption and perception of technology in the Global South. Even among citizens who use internet technology, most are not aware of the full capabilities of their devices. Citizens may be hesitant to trust technology due to criminal hackers, as well as government intrusion. There is also a gender savviness gap in countries where men dominate professions using computers. Economics also play a role, as internet technology is relatively expensive in Global South countries. After these external factors, the ease of use appears to be the biggest impediment to adoption. The technology acceptance model posits that the two factors that immediately influence a person's decision to use new technology are the perceived usefulness and ease of use of technology. This model is illustrated in Figure 1. Generally, people in the Global South already perceive internet technology to be useful. Therefore, when creating a security product, the focus should be on improving perceived ease of use and lowering barriers imposed by external factors.

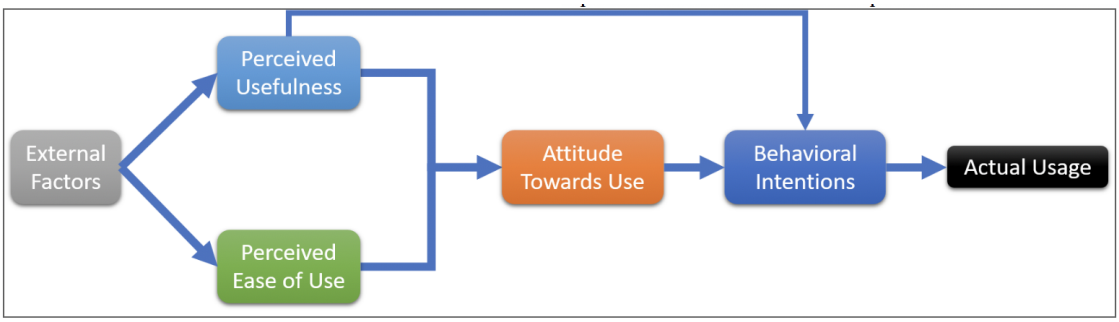

Figure 1. The technology acceptance model.

5.2. Standards for Measuring a Tool's Viability

Correctly setting up and using a security tool can be difficult for any user. How one goes about measuring the factors that contribute to task difficulty is a significant challenge. Task complexity, the requirement to multitask, lack of training, inconsistency of responses to actions, and demands on both long-term and short-term memory will all play a role [34]. Therefore, the simplest, least demanding tool that provides the greatest security is best.

There are a variety of standards for measuring a tool's usability and ease of use. MUSiC (Metrics for Usability Standards in Computing) evaluates the efficacy of a product's use by evaluating the quality of task completion and the time that is required to complete. It also takes into consideration a multitude of context-dependent factors, such as cognitive workload, user satisfaction, rate of learning, time used productively, and effectiveness. While many of these are qualitative and subjective, MUSiC attempts to quantify these values with formulas that produce easily understood scores [35].

QUIM (Quality in Use Integrated Measurement) seeks to integrate multiple standards of measuring usability into one model. QUIM breaks down into 10 usability factors, such as universality, accessibility, and productivity. Each of these factors are evaluated while using 26 criteria, such as time, accuracy, and simplicity. This breaks down into 127 specific metrics for usability. The attractiveness of QUIM is that it avoids the problem of subjectivity, as these metrics can be found by either using a formula or simply by counting. For example, one could measure the amount of processing power that is required to run the program in order to evaluate a program's efficiency [36].

HCI-S (Human Computer Interaction Security) evaluates the user-friendliness of a security system. It is often acknowledged that a system made with usability as a priority will be less secure, and that

high-security systems will be difficult to use. HCI-S proposes six simple criteria that help to find a balance between usability and security: first, the tool should convey security features available to the user in an easily understood format. Second, the security status should be visible to the user. Third, the interface should be easy to learn. Fourth, the design should be minimalistic, only showing what is necessary. Fifth, error messages should be easy to understand and act upon. Sixth, the user should have a satisfactory experience. If all six criteria are met, this leads to trust. It is vital in a security environment that the user trust the tool [37].

5.3. Universality, Simplicity, and Effectiveness

Adopting these standards towards a Global South context would not be a perfect fit. The criteria do not place enough emphasis on external factors, like education and economic status, which are major obstacles in developing countries. They also do not sufficiently account for security fatigue. The threat landscape is ever-changing and new problems are discovered every hour. Therefore, a decent security tool ought to be updated frequently. The users should be able to reasonably expect that a tool will remain effective into the near future.

However, each of these standards express three fundamental factors that are readily applicable to the Global South context. Those are Universality, Simplicity, and Effectiveness (USE). USE highlights the technology adoption problems in the Global South and it provides corrective direction. These three factors each decompose into two or three criteria, which further decompose into two or three binary or quantitative metrics. In short, this is a very simple review.

A table that explains the metrics and how to apply them can be found at the end of this article.

5.3.1. Universality

A defense must serve the largest population possible to be considered as universal. This means it must be classless, multilingual, and portable. Classless means that it can be used by anyone, regardless of educational attainment, economic status, or physical ability. Multilingual means that the tool and its help documentation are available in many languages. Portable means it is compatible with many platforms. It does not require a high-end machine and can be used on the most widely available operating systems (OS). Windows 7 was the most widely used OS in the Global South at the time this study was done [37]. Therefore, a security tool ought to be compatible with Windows 7 to be considered viable in the Global South.

5.3.2. Simplicity

For a tool to be considered simple, it must be minimalistic, green, and effortless. Minimalistic means that the tool only provides necessary features, conveys information clearly, and suppresses irrelevant information. One way to measure this is by counting how many words and features are on the main screen. Green means using nominal system resources, such as processing power, memory, and hard drive space. An effortless tool requires virtually no cognitive effort or decision making on the part of the user. Effort level is determined by a formula that takes simple metrics, such as words of required reading R, time to complete in decimal minutes T, the number of clicks required C, and the number of tasks the user must complete D. This produces a user effort score U. A high score of U corresponds with a higher level of effort. It is assumed that the user will have to read at least one word and click at least once to complete one task.

$$U = \frac{R}{100} \times \left(\frac{C}{D} + T \right) \tag{1}$$

5.3.3. Effectiveness

An effective defense is functional, fixable, and future proof. Functional speaks to the user's intent, and whether the tool solves a problem for the user. In the context of this study, the problem

is either surveillance, censorship, or both. Fixable tools are not error prone, and there is technical support staff or at least a large body of help documentation available for when something goes wrong. Future-proof tools are frequently updated, and the tool's developers can be reasonably expected to continue supporting the tool into the near future.

6. Methodology and Testing

The security tools selected represented a variety of defense types: proxy sites, virtual private networks (VPN), onion networks, encryption software, alternative social media, antivirus software, data wiping software, and security-centric OS. Figure 2 is a chart illustrating which tool type corresponds to thwarting censorship and/or surveillance (targeted and mass).

Tool	Thwarts Targeted Surveillance	Thwarts Mass Surveillance	Thwarts Censorship
Proxy Sites		✓	✓*
VPN	✓†	✓	✓
Onion Routing		✓	✓
Local Encryption	✓		
Alt. Social Media		✓	✓
Antivirus	✓		
Wiping	✓		
Secure OS	✓	✓	

Figure 2. Table showing how a defensive tool corresponds with surveillance or censorship.

Most of these terms are widely understood in the IT industry save for "alternative social media" and "security-centric OS". Alternative social media are online communities and platforms that are privacy-conscious and designed in a way that would frustrate a surveillance state. Security-centric OS are simply OS that are designed with security as the foremost concern, and the user's privacy, anonymity, and safety are prioritized over performance.

Figure 3 is a table of the specific tools that were evaluated with a brief description. They were chosen for their ease of availability and keen following within the information security community.

Tool	Class	Description
Adaware	Antivirus	Antivirus software that requires registration before running.
Aether	Alt. Social Media	A distributed social network that requires a program to be installed on the host system to access.
AxCrypt	Encryption Software	Free software offering AES-128 encryption.
Bleachbit	Wiping Software	Software used for deleting specific files.
DBAN	Wiping Software	A wiping utility that has an automated option.
Ello	Alt. Social Media	A social network targeted towards artistic users.
GnuPG/Kleopatra	Encryption Software	Free encryption software with many features.
I2P	Onion Net	A browser extension that connects to the I2P onion network.
K Proxy	Proxy Site	A free proxy site with many servers to choose from.
Malwarebytes	Antivirus	Free antivirus software that is widely used.
Qubes	Secure OS	A unique OS that compartmentalizes processes.
Skull Proxy	Proxy Site	A very minimalistic proxy site.
Tails	Secure OS	An OS that does not have persistent storage.
Tor Browser	Onion Net	A browser that only connects to the Tor network.
TunnelBear	VPN	A VPN that allows users to connect to many different countries.
Windscribe	VPN	A VPN that offers 10GB of data per month for free.

Figure 3. Tools that were tested for this study.

6.1. Method

Each tool, save for Qubes and DBAN, was individually tested on an ASUS N61J laptop running Windows 7 Home Premium. Qubes and DBAN were tested on a custom desktop. The process of setting up and running each tool once was recorded, and then reviewed against USE metrics. Documentation from tool developers was analyzed using the Flesch–Kincaid Grade Level test in order to determine the approximate education level that is required to use each tool [36]. In cases where information was not found in the tool itself, developers' pages were also reviewed to discover cost, system requirements, available languages, accessibility options, technical support options, and date of last update.

Each metric earns a point. In any cases where a metric would not be applicable (such as the window size of a fully adjustable window), that point is not lost. Credit was also given in cases where developers expressed that accessibility options would be a priority in a future update, even if the current version of the tool did not have accessibility options. The U score can impact the simplicity score. The total score is the average of the three subscores of Universality, Simplicity, and Effectiveness. The overall score is also an F if the tool scores an F in any of those three sections.

6.2. Finding U

This study primarily looks at two types of tools: ones that require downloading and installing a program, or ones that are only interacted with through a browser. Successfully using a security program requires navigating to the web page where the program is hosted, downloading it, installing it, and running it at least once. Navigating, downloading, installing, and running counts as four tasks ($D = 4$). Successfully using a browser-based tool requires navigating to the site, setting up an account (if necessary), and running the tool. Navigating, account setup, and running counts as three tasks ($D = 3$). Ideally, a task should be completed in one click. Any words that the user must read to complete the task (such as "download here") are counted as required reading. End user license agreements are not included in required reading. Time is in decimal minutes, which is the total number of seconds divided by 60. Exceedingly long periods of downloading or scanning are not included in T. Naturally, different types of tools require different levels of user effort, so it should be unsurprising if a proxy site has a significantly lower U score than an OS. However, a U score that exceeds 100 is considered too difficult and, therefore, not viable.

7. Results

The USE scores for each of the 16 tools are found in Figure 4. While mostof the tools were found to be effective, they lacked sufficient universality and simplicity to be considered viable. Hence, six (37.5%) of the tools failed the review. The operating systems Qubes and Tails OS both demanded significant cognitive effort to setup, required a large amount of reading, and both had high hardware requirements. While the proxy sites KProxy and Skull Proxy were very easy to use, neither had help documentation or support staff, and it is unclear when they were last updated. KProxy does not work with every website and it requires some troubleshooting to use successfully. Kleopatra, the encrypting software, has an incredibly complicated interface and requires a good deal of effort to understand. The alternative social network, called Aether, is defunct and no longer supported.

Open Issues

The best performing tools were the Tor Browser, Windscribe, TunnelBear, and AxCrypt. Each of these tools is easy to setup and has a very minimalistic interface. Each of them can be operated in multiple languages, and they also offer help documentation in many languages. There is also support staff available for each one. All four were updated within a six-month period and they can be reasonably expected to remain supported for the near future.

Tool	Universality	Simplicity	Effectiveness	U Score	Overall Grade
Tor Browser	B-	A-	A+	3.612	**A**
Windscribe	**A-**	**B**	**A+**	4.512	**A**
TunnelBear	A	B-	A+	9.45	**A**
AxCrypt	A-	B-	A+	5.456	**A-**
Ello	C	A-	A+	2.773	**B+**
Bleachbit	C-	A	A+	1.457	**B**
Malwarebytes	B-	D-	A+	3.24	**B-**
Adaware	**C**	**D-**	**A**	5.428	**C+**
I2P	B-	D+	A	31.357	**C+**
DBAN	D-	D+	D	28.432	**D**
Tails OS	C-	F	A+	**374.185**	**F**
GnuPG/Kleo.	A	F	B-	67.485	**F**
Qubes	F	F	B-	**106.079**	**F**
Skull Proxy	D-	A+	F	0.027	**F**
Aether	C-	B-	F	2.128	**F**
K Proxy	D-	C-	F	0.335	**F**

Figure 4. Table of results.

As anticipated, many of these tools have high education requirements. The Flesch–Kincaid Grade Level test results of each tools' documentation can be found in Figure 5. This is an obstacle to adoption, and it hinders the user's ability to understand the tool, how it works, and how to troubleshoot it. A classless security tool should not require a high degree of education attainment, especially in a Global South context, where many do not attend school for more than a few years. Improving the readability of a tool's documentation would significantly widen the audience that can use that tool. While most of the tools operate in more than one language, only seven (43.75%) offer help documentation in multiple languages. Translating help documentation into multiple languages greatly expands the number of people who can effectively use and troubleshoot the tool. There appears to be a slight correlation between offering help documentation in multiple languages and good effectiveness scores. It may be that offering more languages expands the user base, which incentivizes the developers to update their tools more often.

Some tools required additional steps that seemed to be excessive. Four (25%) of the tools require using third party software to setup. It would be better if everything that was required for the setup was packaged into a single executable. AxCrypt and Adaware both require registering by email, although it is unclear why that is necessary or how it benefits the user. These additional tasks further complicate what could otherwise be a simple setup process.

Only four (25%) of the tools tested had accessibility options for physically impaired users or promised to provide accessibility options in a future update. This means impaired users would have to rely on third-party software to use most tools. This software can be expensive and it is not always compatible with other tools. Poverty and poor healthcare are endemic to the Global South and, therefore, native accessibility options are important for users in these areas.

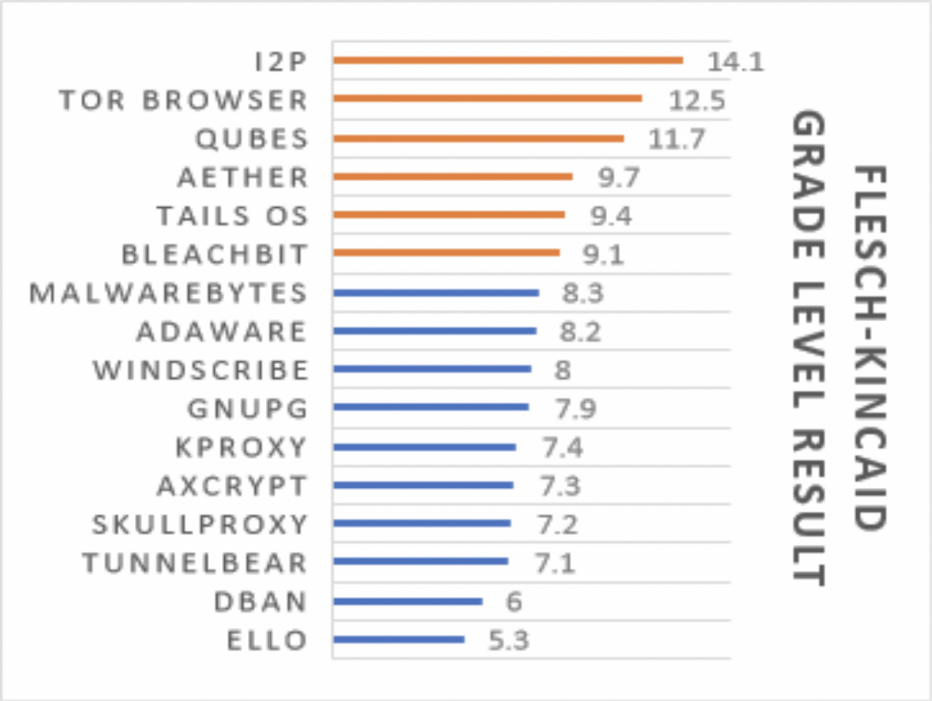

Figure 5. Flesch–Kincaid Grade Level test results.

There are limitations to the USE metrics that became clear as the study was being conducted. Some tools prioritize offering the user many features and a great deal of modularity. This negatively impacts simplicity and minimalism, even if some users would prefer a more flexible program. Additionally, some factors should be considered to be more important than others. For example, there are more users who would benefit from a multilingual platform without accessibility options than an English-only platform with accessibility options. It is also natural to expect that more complicated security systems will require greater user effort to setup. A high U score may be forgivable if the product is extremely effective in other ways. Therefore, future study would require revamping USE to reflect a product's value to the Global South more accurately or adopting a different metric entirely.

Access to these tools is another challenge. In some countries, it may be illegal to use them, and authoritarian governments could implement controls preventing citizens from obtaining them. Evaluating access to a security tool would need to be done on both a per-country and per-end user basis, because the laws and practices of each country are different. A tool that is illegal in one nation will be legal in another. Within a nation, it may be permissible for everyone to use a tool, except a persecuted minority. Figure 6 shows a complete list of all the parameters used in this study.

Mobile devices were not a part of this study. However, as their use in the Global South continues to grow, the need for a study in that area is becoming apparent. Mobile devices are notoriously insecure and mobile apps can be a vector for malware. Telecommunication companies may be subject to government oversight, which is another avenue for surveillance or censorship. Therefore, future study in this area should include a review of mobile security tools.

Universal	Classless	Cost	This is the price of the product. Anything other than free loses this point.
		Reading Level	This is the Flesch-Kincaid Grade Level of either an instructional manual, FAQ, or some other product documentation in English, as determined by an automated system. [80] Anything scoring 9 or greater loses this point.
		Accessibility	A tool is accessible if it can be used by the differently-abled, such as hard-of-sight or hard-of-hearing users. If no such attempt is made, this point is lost.
	Multilingual	English Only	This is a binary, yes or no metric on whether the tool is only available in English. If yes, the point is lost.
		# of Operating Languages	This number reflects how many different languages the tool can be run on. Less than five loses a point.
		# of Help Documentation Languages	This number reflects how many different languages help documentation can be found in. Less than three loses a point.
	Portable	Windows 7	This is a binary, yes or no metric on whether the tool is compatible with Windows 7. If no, the point is lost.
		# of Operating Systems	This number reflects how many operating systems the tool is compatible with. Less than two loses a point.
		Hardware Requirements	This is simply the CPU, RAM, and HDD requirements to use the tool. Relatively high requirements lose the point.
Simple	Effortless	# of Tasks (D)	This is how many tasks a user must complete to successfully set up and use the tool at least once. The point is lost if D ≥ 5.
		# of Clicks (C)	This is how many times the user must click a mouse button to successfully set up and use the tool at least once. When filling out forms, each field is counted as one mouse click. The point is lost if C > 25.
		# of Words (R)	This number reflects how many words a user must read to successfully set up and use the tool at least once. The point is lost if R > 100.
		Time in Decimal Minutes (T)	This number reflects the total amount of time it takes a user to set up and use the tool at least once. The point is lost if T > 5.
		U Score	This number reflects the cognitive effort required to set up and use the tool at least once, and is found using the following formula: $\mathbf{U} = \frac{\mathbf{R}}{100} \times \left(\frac{\mathbf{C}}{\mathbf{D}} + \mathbf{T}\right)$ If U < 5, the simplicity score is improved one level (A → A+). If U > 10, the score is reduced one level (A- → B+). If U > 100, the simplicity score is F.
	Minimalistic	Main Window Size	This is the size of the tool's main window in pixels. If the total size exceeds 800 x 600, the point is lost.
		Can Run in Background	This is a binary, yes or no metric on whether the tool can be run in the background or if it needs continuous user attention. If no, the point is lost.
		# of Visible Features	This number reflects how many features are available in the main window. The point is lost if there are more than 10.
		# of Words on Screen	This number reflects how many words appear in the main window. The point is lost if there are more than 25.
	Green	Resource Requirement	This number reflects how much processing power and memory are used while the tool is running. The points are lost if it is excessively high.
Effective	Functional	Solves Problem	This is an evaluation of whether the tool serves the user's end goals. It is a binary, pass or fail metric. In this case, the tool passes if it thwarts surveillance or censorship. If it does neither, it is an automatic fail in effectiveness.
	Fixable	Help Documentation Available	This is a binary, yes or no metric on whether help documentation is available for this tool. The point is lost if there is none.
		Support Staff Available	This is a binary, yes or no metric on whether human technical support is available to the user should a problem arise. If no, the point is lost.
		Troubleshooting Requirement	This is a binary, yes or no metric on whether something went wrong during first time setup and required troubleshooting. The point is lost if there was a problem.
	Future Proof	Still Supported	This is a binary, yes or no metric on whether the developer still supports the tool. The point is lost if it is no longer supported.
		Date of Last Update	This is the most recent date the tool was updated. An excessively long period of time or failure to report the last update results in a lost point.

Figure 6. Parameters for our study.

8. Conclusions

The goal of this discussion is to enhance the understanding of challenges to technology adoption in the Global South in the context of persecution and oppression. To that end, this article concludes that the current offering of defensive measures is insufficient. While most of these tools are technically fit-for-purpose in terms of thwarting censorship and surveillance, they serve a narrow audience and are not viable for the people who would benefit from them the most.

Ease of use and external factors are the primary barriers to security tool viability in the Global South. There is admittedly little a developer can do to ease the pressures of external factors such as low income or unjust laws. However, tools that are more universally usable and simpler will ultimately be the most accessible. The prescriptive recommendations based on this evaluation are:

- Security tools should be available in at least five languages to reach the largest audience possible.
- A security tool must have accessibility options that enable hard-of-sight and hard-of-hearing users to use the tool.
- The interface for the tool should be uncluttered and easily navigable. Communicate the most amount of information possible with the least amount of words possible.
- Provide meaningful updates as frequently as possible. This keeps the tool viable and engenders trust between the tool and its users.
- Keep the number of setup steps that are required as small as possible. The fewer actions a user must perform, the more likely it is the user will use the tool successfully.

Internet use carries significant risk in persecuting societies. Users in the Global South face the most danger, as they do not possess the social power to dictate how their internet use is monitored or regulated. It is imperative that these users have access to cybersecurity tools that are universal, simple, and effective. Defeating digital persecution in the Global South today would save four-billion people from serious hardship tomorrow.

Author Contributions: Conceptualization, L.E.P. and T.H.; methodology, L.E.P.; software, L.E.P.; validation, L.E.P.; formal analysis, L.E.P.; investigation, L.E.P.; resources, L.E.P., abd T.H.; data curation, L.E.P.; writing–original draft preparation, L.E.P.; writing–review and editing, L.E.P. and T.H; supervision, T.H.; project administration, T.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Arora, P. The Bottom of the Data Pyramid: Big Data and the Global South. *Int. J. Commun.* **2016**, *10*, 1681–1699.
2. Ali, A.I. Citizens under Suspicion: Response Research with Community under Surveillance. *Anthropol. Educ. Q.* **2016**, *47*, 78–95. [CrossRef]
3. Standard Country or Area Codes for Statistical Use (M49). United Nations. Available online: https://unstats.un.org/unsd/methodology/m49/ (accessed on 15 April 2020).
4. Kshetri, N. Big data's impact on privacy, security and consumer welfare. *Telecommun. Policy* **2014**, *38*, 1134–1145. [CrossRef]
5. Amnesty International. *Human Rights Defenders Under Threat—A Shrinking Space for Civil Society*; Amnesty International: New York, NY, USA, 2017.
6. *The Global Surveillance Industry*; Privacy International: London, UK, 2016.
7. Nabi, Z. *The Anatomy of Web Censorship in Pakistan*; Information Technology University: Punjab, Pakistan, 2013; Available online: http://0b4af6cdc2f0c5998459-c0245c5c937c5dedcca3f1764ecc9b2f.r43.cf2.rackcdn.com/12387-foci13-nabi.pdf (accessed on 8 July 2020).
8. Rice, S.; Geels, K.; Hackett, H.R.; Trafimow, D.; McCarley, J.S.; Schwark, J.; Hunt, G. The Harder the Task, the More Inconsistent the Performance: A PPT Analysis on Task Difficulty. *J. Gen. Psychol.* **2012**, *139*, 1–18. [CrossRef] [PubMed]
9. A Fall to Cheer. *The Economist*, 3 March 2012. Available online: http://www.economist.com/node/21548963 (accessed on 10 July 2020).
10. Moore, R.I. *The Formation of a Persecuting Society: Authority and Deviance in Western Europe 950–1250*, 2nd ed.; Blackwell: Malden, MA, USA, 2007.
11. republica2010, re:publica 2012—Eben Moglen—Freedom of Thought Requires Free Media. YouTube, 19 May 2012. Available online: https://www.youtube.com/watch?v=sKOk4Y4inVY (accessed on 10 July 2020).
12. Gurses, S.; Kundnani, A.; Van Hoboken, J. Crypto and empire: The contradictions of counter-surveillance advocacy. *Media Cult. Soc.* **2016**, *38*, 576–590. [CrossRef]

13. Sokefeld, M.; Strasser, S. Introduction: Under suspicious eyes–surveillance states, security zones and ethnographic fieldwork. *Z. Ethnol.* **2016**, *141*, 159–176.
14. Warf, B. Geographies of Global Internet Censorship. *GeoJournal* **2011**, *76*, 1–23. [CrossRef]
15. The World Factbook. Central Intelligence Agency, 1 April 2016. Available online: https://www.cia.gov/library/publications/the-world-factbook/ (accessed on 24 July 2020).
16. Baquero-Hernandez, R.A. Characterizing E-Government in China. *Desafios* **2012**, *24*, 233–257.
17. Dong, F. Controlling the internet in China: The real story. *Converg. Int. J. Res. Into New Media Technol.* **2012**, *18*, 403–425. [CrossRef]
18. Marczak, B.; Weaver, N.; Dalek, J.; Ensafi, R.; Paxson, V. An Analysis of China's "Great Cannon". 2015. Available online: https://citizenlab.ca/2015/04/chinas-great-cannon/ (accessed on 17 July 2020).
19. Chandel, S.; Jingji, Z.; Yunnan, Y.; Jingyao, S.; Zhipeng, Z. *The Golden Shield Project of China: A Decade Later—An in-Depth Study of the Great Firewall*; International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC); IEEE: Guilin, China, 2019, pp. 111-119. [CrossRef]
20. Qin, B.; Stromberg, D.; Wu, Y. Why Does China Allow Freer Social Media? Protests versus Surveillance and Propaganda. *J. Econ. Perspect.* **2017**, *31*, 117–140. [CrossRef]
21. Amnesty International. *Death Sentences and Executions 2014*; Index: ACT 50/001/2015; Amnesty International: New York, NY, USA, 2015.
22. Karagiannopoulos, V. The Role of the Internet in Political Struggles: Some Conclusions from Iran and Egypt. *New Political Sci.* **2012**, *34*, 151–171. [CrossRef]
23. Gupta, R.; Muttoo, S.K. Internet Traffic Surveillance & Network Monitoring in India: Case Study of NETRA. *Netw. Protoc. Algorithms* **2016**, *8*. [CrossRef]
24. Berman, I. Iranian Devolution: Tehran Fights the Digital Future. *World Aff.* **2015**, *178*, 51–57.
25. Ahmed, A.; Perlroth, N. Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families. *The New York Times*, 19 June 2017. Available online: https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html(accessed on 23 July 2020).
26. Escaping from North Korea in Search of Freedom | Yeomni Park | One Young World. YouTube, 18 October 2014. Available online: https://www.youtube.com/watch?v=ufhKWfPSQOw (accessed on 17 July 2020).
27. Sedaghat, N. North Korea Exposed: Censorship in the World's Most Secretive State. 17 March 2014. Available online: https://web.archive.org/web/20150509050318/ (accessed on 17 July 2020).
28. Haque, J. Pakistan's Internet Landscape: A Report by Bytes for All, Pakistan. 2013. Available online: https://new.waccglobal.org/wp-content/uploads/wacc-global/Images/Articles/2014/01Jan/Pakistan-Internet-Landscape.pdf (accessed on 28 September 2020)
29. UIS Unesco. Mean Years of Schooling. Available online: http://data.uis.unesco.org/ (accessed on 23 June 2020).
30. Ejiaku, S.A. Technology Adoption: Issues and Challenges in Information Technology Adoption in Emerging Economies. *J. Int. Technol. Inf. Manag.* **2014**, *23*, 59–68.
31. Alssbaiheen, A.; Love, S. Exploring the Challenges of M-Government Adoption in Saudi Arabia. *Electron. J. Gov.* **2015**, *13*, 18–27.
32. Okyere-Kwakye, E.; Nor, K.M.; Ologbo, A.C. Technology Acceptance: Examining the Intentions of Ghanian Teachers to Use Computer for Teaching. *Afr. J. Libr. Arch. Inf. Sci.* **2016**, *26*, 117–130.
33. Bevan, N. Measuring usability as quality of use. *Softw. Qual. J.* **1995**, *4*, 115–150. [CrossRef]
34. Seffah, A.; Donyaee, M.; Kline, R.B.; Padda, H.K. *Usability Measurement: A Roadmap for a Consolidated Model*; Universite de Lausanne: Lausanne, Switzerland, 2009.
35. Johnston, J.; Eloff, J.H.P.; Labuschagne, L. Security and human computer interfaces. *Comput. Secur.* **2003**, *22*, 675–684. [CrossRef]
36. Desktop Windows Versions Market Share Worldwide. StatCounter: GlobalStats. Available online: http://gs.statcounter.com/os-version-market-share/windows/desktop (accessed on 28 July 2020).
37. Readable.io. Available online: https://readable.io/ (accessed on 12 August 2020).