William R. Marczak* and Vern Paxson

Social Engineering Attacks on Government Opponents: Target Perspectives

Abstract: New methods of dissident surveillance employed by repressive nation-states increasingly involve socially engineering targets into unwitting cooperation (e.g., by convincing them to open a malicious attachment or link). While a fair amount is understood about the nature of these threat actors and the types of tools they use, there is comparatively little understood about targets' perceptions of the risks associated with their online activity, and their security posture. We conducted in-depth interviews of 30 potential targets of Middle Eastern and Horn of Africa-based governments, also examining settings and software on their computers and phones. Our engagement illuminates the ways that likely targets are vulnerable to the types of social engineering employed by nation-states.

Keywords: privacy, human rights, surveillance

DOI 10.1515/popets-2017-0019
Received 2016-08-31; revised 2016-09-30; accepted 2016-10-01.

1 Introduction

Recent work developed evidence that activists, NGOs, and civil society are targeted with abusive surveillance from nation-states and other well-resourced attackers. Due to increasing use of encryption, and attackers' desire to target beyond their borders, such surveillance frequently moves beyond passive methods, and includes hacking targets' *devices*, to deanonymize them or exfiltrate private information. Such hacking often involves a *social engineering* component as a first step, where an operator tries to convince a target to open a malicious artifact, such as a link or attachment, included in a message. For instance, the operator may pose as the target's friend, an organization with which the target has a relationship, or a new contact that claims to be providing information of interest to the target. Once opened, the link or attachment may attempt to profile the target's devices, or infect them with spyware. In some cases, these types of surveillance involve the use of products or services furnished by commercial "lawful interception" vendors.

While it is understood that activists, NGOs, and civil society targets are at risk for surveillance, and popular methods of compromise have been extensively documented [1–3], far less is known about how such groups perceive surveillance risks, any relevant training they have received, and how their perceptions and knowledge, along with their dissident activities, shape their security behaviors and risks. To devise effective surveillance defenses for targeted groups, we need to first interact with such groups in detail.

We engaged with 30 targets, on the ground in two Middle Eastern countries, as well as Middle East and Horn of Africa diaspora members overseas, through in-depth (IRB-approved) structured cybersecurity interviews. While the subjects we interviewed reflect the behavior of ordinary users in a number of ways, we also find important differences in terms of the subjects' perceptions of risk (surveillance resulting in government punishment was feared by more than half of on-the-ground activists) and specific security behaviors, such as using out-of-country human "password managers" (Section 3.7) to maintain security of online accounts.

Despite their heightened awareness of risk and steps taken in response to it, on the whole however our results indicate that activists, NGOs, and civil society remain vulnerable to attacks involving social engineering. For example, while subjects reported performing basic vetting before interacting with links and attachments—such as checking the sender ($>$ 2/3 of subjects), or evaluating the context of the message ($>$ 1/3)—this sort of checking can still prove vulnerable to subtle social engineering, including sender spoofing and "doppelgänger" accounts. This threat particularly looms for attackers with access to a friend or contact's compromised (or seized) account, and indeed 40% of subjects had no strategy to recover their compromised accounts, and 57% reported no strategy if they lost their phone.

Even subjects who report positive security behavior can come up short in implementing it correctly. One subject we interviewed who reported checking a message's sender and context for vetting contacted us several weeks after the interview, stating that he had opened an attachment from an email that he later realized was sent from an account designed to impersonate one of his friends. The attachment was benign, but a link included in the email contained spyware. Overall, com-

***Corresponding Author: William R. Marczak:** UC Berkeley, Citizen Lab, E-mail: wrm@cs.berkeley.edu
Vern Paxson: UC Berkeley, ICSI, E-mail: vern@icir.org

paratively fewer subjects reported using tools such as online scanning tools on links or attachments they received, or following up with a message's purported sender through another means of communication before interacting with the message.

Section 2 introduces related work, Section 3 presents our survey methodology, results, and takeaways. We conclude and outline future research directions in Section 4.

2 Related Work

Social engineering of civil society. Previous academic work illustrates targeted nation-state social engineering of activists and civil society [1–3]. Attackers include government agencies themselves, cyber mercenaries (hackers for hire), and cyber militia groups. Tools used by attackers include malware, exploits, and links sent to pseudonymous accounts that record a clicker's IP address to aid deanonymization by a government. In some cases, attackers use malware purchased from commercial "lawful intercept" vendors such as FinFisher [4], Hacking Team [5], and NSO Group [6]. In other cases, attackers write malware themselves, or employ common Remote Access Trojans (RATs) developed by the cybercrime underground.

In addition, substantial leaked data from FinFisher [7] and Hacking Team [8] reveals product functionality and the operation of surveillance markets. While convincing a target to open a malicious link or file (either with or without an exploit) is a a main vector advertised by these companies, they also offer stealthier infection options including *network injection* hardware, which can be installed on an ISP's backbone to inject malware in targets' unencrypted Internet connections [9, 10].

Previous work also indicates that attackers shift tactics in response to targets' security behaviors. For instance, targets who employed two-factor authentication received specially designed phishing crafted to capture both passwords and authorization codes [11], and a campaign urging Tibetan activists to "detach from attachments" [12] led attackers to instead distribute malicious files via Google Drive links [13].

Studies of user security behavior. Previous work has studied user security behaviors generally, as well as among specific groups. For instance, McGregor et al. [14] studied digital security practices of American and French journalists, a group that reported facing somewhat similar risks to our subjects (e.g., prison, physical danger, and discovery of identity). Authors conducted 15 in-depth interviews, focusing in particular on how journalists' workflows influence their behaviors and use of security tools. Authors noted that several interviewees employed *ad hoc defensive strategies* that sometimes introduced additional vulnerabilities, a finding we share. In contrast, our study focuses primarily on the documented threat of targeted attacks through malicious messages, rather than surveillance more broadly.

Some examples of work studying more general subject populations are Forget, et al. [15], and the *AOL/NCSA Online Safety Study* [16]. In [15], the authors enlisted subjects to install a monitoring agent on their computers to transmit their behavior to researchers for analysis. While the study identified some similar security deficiencies as ours (e.g., lack of security software, out-of-date operating systems and plugins such as Adobe Flash), their subject population (recruited via a university service) likely faces different risks than ours.

In [16], the authors interviewed a sample of 329 adult Internet subscribers in 2004, selected by an "independent market analysis organization" in 22 different American cities and towns. They asked subjects a variety of questions, including how safe subjects felt their computer was from "viruses," "hackers," and "online threats," whether subjects employed antivirus software and firewalls, and how often they updated these. The authors then ran a "scan" of each subject's computer, to verify whether antivirus software and firewalls were present, correctly configured, and up-to-date. A majority of their subjects felt "very safe" or "somewhat safe" from "online threats" (77%), "viruses" (73%), and "hackers" (60%), whereas we classified only 47% of our subjects as believing that their "online activities" placed them at "low risk" (Section 3.3). The authors also found that 85% of subjects had antivirus software installed (83% thought they did), though only 33% had virus definitions that were up-to-date (within a week), and 12% had definitions older than six months. Among our subject population, 72% of computers had antivirus software installed, and 14% of installed antivirus software was not up-to-date (in all cases because the update subscription had expired); the discrepancy in update rates may be due to the increasing prevalence (since 2004) of default automatic updates in antivirus programs, and OS warnings if antivirus software is not configured.

It is worth noting that our population is significantly more specialized than general survey populations, such as the sample interviewed by Northwestern University's 2015 *Media Use in the Middle East* survey [17], which polled more than 6,000 Internet users in six Middle Eastern countries about censorship, surveillance, and other issues. Overall, 38% of individuals were "worried about governments checking what I do online." In comparison, we found that 28/30 subjects were concerned about at least one government targeting them.

Defenses for social engineering. Significant prior work has looked into detecting *phishing*, e.g., messages that induce users to supply account credentials to a website, by examining a wide range of features, including page structure and network characteristics [18], and visual presentation [19]. We also note that civil society invests significant resources in provid-

ing digital security trainings for at-risk populations (e.g., [20]), though the efficacy of such training in reducing compromise is an open question.

3 Survey

Our survey blended interview questions regarding subjects' perception of risk and security behaviors with examination of their computers and phones. After concluding our intervention with a subject, we offered to answer any additional subject questions, and provided them with customized security advice (subjects were not paid for their participation). Subjects asked about the safety of specific chat apps, the capabilities that governments were likely to employ against them, as well as more general technical questions including how to recover deleted files. We describe our survey methodology in Section 3.1, present results in Sections 3.2–3.8, and identify key take-aways in Section 3.9.

3.1 Methodology

We interviewed thirty subjects (randomly assigned identifiers S_1–S_{30}) over a two year period between March 2014 and March 2016. We conducted Interviews in two GCC[1] countries, as well in the United States and United Kingdom, where we interviewed human rights workers, and activists originally from the GCC and Horn of Africa (HoA) but now residing abroad.

We obtained verbal consent (in GCC countries) and signed consent (in the US and UK) before proceeding. Consent materials were available in both Arabic and English. All interviews were conducted in English, with the exception of two interviews in GCC countries, which were conducted with translation aid provided by an Arabic speaker proficient in the local dialect.

While in the GCC, we rigidly practiced careful IRB-approved operational security. To protect participants' identities and responses, we implemented IRB-approved measures to reduce our susceptibility to remote tracking, and minimize the amount of information that authorities could recover if we were arrested and forced to reveal passwords while in-country. To avoid stealthy physical compromise, we implemented procedures to determine whether our electronic devices had been subject to surreptitious tampering or inspection.

We recruited GCC-based subjects through trusted activist connections on the ground, who invited potential subjects they believed to be at risk of government surveillance. All interviews in the GCC were conducted at a place of the subject's choosing, and we abided by all conditions set by contacts (e.g., one subject requested that we carry on a fictitious conversation suggesting we were old friends while traveling in his vehicle, until we had reached a location where he was comfortable talking freely).

We recruited subjects outside of the GCC by reaching out to our contacts in civil society and human rights organizations.

3.2 Demographics

Four subjects were from a global human rights organization, (H), eight were local GCC activists, (G), eight were GCC activists living abroad, (D), and ten worked at an out-of-country Horn of Africa (HoA) media outlet, (M).

Throughout the interview, we asked subjects basic demographic questions (Table 1), including whether they had received formal digital security training (**Received training**). The vast majority (>2/3) of subjects had not received formal digital security training. Two subjects mentioned that they provided digital security trainings for others, including one who had not received training themselves.

Table 1. Demographics of study groups

	(H)	(G)	(D)	(M)	Total
Female:male	2:2	0:8	3:5	1:9	6:24
Median age	46	31.5	39	38	38
Received training	4/4[2]	2/8[3]	2/8[4]	1/10[5]	9/30
Provided training	0/4	2/8	0/8	0/10	2/30
Highest level of education					
High school	0/4	0/8	1/8	1/10	2/30
Associates	0/4	0/8	0/8	1/10	1/30
High Diploma[6]	0/4	2/8	1/8	0/10	3/30
Bachelors	0/4	2/8	2/8	5/10	9/30
Masters	1/4	3/8	2/8	2/10	8/30
Doctorate	3/4	1/8	1/8	1/10	6/30

While we did not ask a specific question about whether respondents had suffered consequences that they believed were linked to their online activity, seven individuals (23%) volunteered this information during the course of the interviews. Three individuals from (G) reported that they had suffered

1 Gulf Cooperation Council: Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, UAE.

2 Three were trained by (H), one by Tactical Tech [20].

3 Both trained by same local activist.

4 One trained by NED [21], one trained by Front Line Defenders [22].

5 InterNews USA [23] and Google.

6 One year less than a Bachelors degree.

such consequences. One activist (S_2) had been subjected to physical assault. One subject (S_{29}) served a year in prison, and upon his release, found that his Twitter password had been changed. One subject (S_9) was sacked from his job. Two individuals from (D) cited hacking of their email and social media accounts (S_{16}, S_{21}). One subject from (M) (S_{11}) reported receiving threats from authorities: *"I was in* [HoA Country] *last year, authorities told me to leave or die, so I left."* One subject from (M) (S_{22}) reported that his Facebook account was hacked, and hackers posted messages stating that he was working with his country's government. The same subject also reported that a copy of a book he was writing was leaked online (he speculated hacking of the computer or email account of him or his friend he had shared a copy with). The same subject also reported in-country harassment of his brother.

3.3 Surveillance risks

To understand perceptions of government targeting, we asked subjects about risks they associated with their online activity, as well as what sorts of attackers they felt might target them online, and to what extent they believed a government was tracking their activities. The overwhelming majority (93%) of subjects mentioned potential government attackers, and 90% indicated the likelihood of the government tracking their online activities to be 50% or greater.

We first asked: *"To what degree do you believe your online activities are safe or place you at risk?"* (Table 2). Two answered that they did not know. We classified the rest of the answers into two categories, **High risk** (e.g., *"at risk," "high risk," "70% unsafe"*), and **Low risk** (e.g., *"variable," "50%," "light risk."*)

We next asked subjects, *"What are the risks?"* (Table 2). One subject responded that they did not know. Based on subject responses, we devised eight categories: **Surveillance**, which includes answers that cited surveillance of, or theft of private information from computers, phones, or online accounts; **Punishment**, which includes denial of due process, arrest, prison, or physical assault; **Publicity**, which includes smear campaigns, blackmail, or any public disclosure of private information; **Friends**, which includes targeting friends, family members, or contacts; **Financial**, which includes theft of financial information; **Access**, which includes travel bans or deportation; **Damage**, which includes damage to devices or loss of data, and **Cloud**, which includes concern about sharing data with cloud providers.

We then asked *"Who do you believe might be targeting you due to your online activities?"* If they did not mention a government actor, we asked them *"Do you think you might be targeted by the government?"* 28 respondents were concerned about at least one government targeting them (Table 3); one was not concerned about government targeting, but was concerned about targeting by private actors aligned with the government (**Pro-gov**). One respondent (from (M)) was unsure who might be targeting them.

Table 2. Subject perception of risks

	(H)	(G)	(D)	(M)	Total
High risk	2/4	3/8	6/8	5/10	16/30
Light risk	2/4	5/8	2/8	3/10	12/30
Risks					
Surveillance	4/4	3/8	7/8	6/10	21/30
Punishment	0/4	5/8	1/8	1/10	6/30
Publicity	1/4	2/8	2/8	0/10	5/30
Friends	0/4	1/8	1/8	2/10	4/30
Financial	0/4	0/8	0/8	2/10	2/30
Access	0/4	2/8	0/8	0/10	2/30
Damage	0/4	0/8	0/8	2/10	2/30
Cloud	0/4	0/8	0/8	1/10	1/30
Total	4/4	8/8	8/8	9/10	29/30

Table 3. Subject perception of attackers

	(H)	(G)	(D)	(M)	Total
GCC gov	0/4	7/8	8/8	0/10	15/30
HoA gov	0/4	0/8	0/8	9/10	9/30
Other gov[7]	4/4	1/8	5/8	0/10	10/30
Pro-gov	0/4	4/8	1/8	2/10	7/30
Others	1/4[8]	1/8[9]	2/8[10]	0/10	4/30

We asked subjects to rate the likelihood of the governments they mentioned tracking their online activities on a scale from one to five (Figure 1).

3.4 PC security

We examined subject PCs (and mobile devices, per Section 3.5) to see if they exhibited well-known security deficiencies, such as issues with security software, or old versions of plugins. We found that 27% of PCs had no security software, 14% of PCs had expired security software, and 27% of PCs had an old version of Adobe Flash, a common exploit vector for social engineering attacks involving malicious documents.

7 Subjects mentioned governments of countries where they lived, and other countries where they worked.

8 One subject cited nongovernmental actors that were the targets of their investigations.

9 One subject mentioned "other groups."

10 One subject mentioned "everybody," another subject mentioned "others."

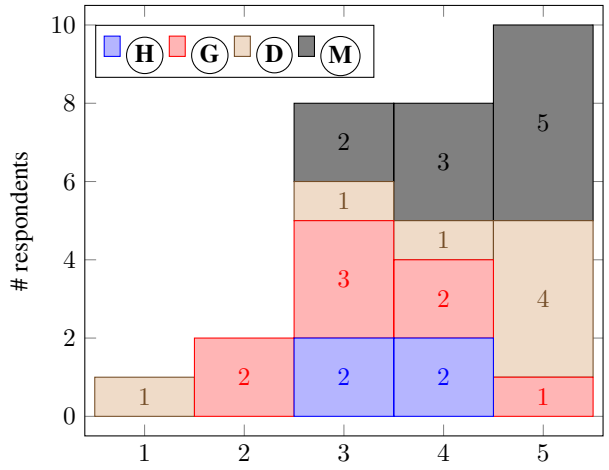

Fig. 1. "How likely is it that the government is tracking your online activities?" (1: definitely not; 5: definitely)

Of the 29 computer users (S_9 from (G) reported they used an iPad instead of a computer), we were able to examine a total of 22 operating systems on 21 computers (one computer each of 21 subjects who had their computer with them at the interview). We examined seventeen Windows computers (and an Ubuntu partition on one of these), 3 OSX computers, and one Linux computer.

Table 4. PC security deficiencies

	(H)	(G)	(D)	(M)	Total
No encryption	0/4	5/6	4/5	7/7	16/22
No AV	0/4	3/6	1/5	2/7	6/22
Expired AV	0/4	2/6	1/5	0/7	3/22
Old Flash	1/4	1/6	1/5	3/7	6/22

19 operating systems had Adobe Flash installed. 13 were selected to allow Adobe to automatically install Flash updates (two of these were 991 and 1,064 days out-of-date; we are unsure why). Four Flash installations were set to prompt the user before installing an update (28, 63, 116, and 273 days out-of-date), and two Linux systems had Flash installed through their respective package managers. We denote out-of-date Flash versions as **Old Flash** in Table 4.

Of the six operating systems (OSes) we investigated that did not appear to have any antivirus (AV) software (**No AV**), two ran Linux, one ran OSX, and three ran Windows. Three additional operating systems had only an expired AV program (**Expired AV**), which was McAfee in each case. While advanced targeted threats may be engineered to evade antivirus software, these products can help protect against some more common threats [24].

The vast majority of operating systems (73%) did not have disk encryption enabled (**No encryption**). Of the OSes with encryption enabled, four were Windows using BitLocker (a company policy at (H)), one was OSX using FileVault, and one was Linux using DM-Crypt.

3.5 Mobile device security

We examined subject mobile phones to check for issues including lax security settings that can ease social engineering (sideloading, rooting), outdated OS versions that can increase odds of successful compromise, and physical security concerns (passwords, encryption, contingency plans for lost devices) that can lead to theft of data or compromise of online accounts by obtaining physical access to a device. We also asked subjects about security behaviors including use of security apps, and responses to application permissions dialogs. We found device physical security to be the area of greatest concern: 68% of subjects did not have an encrypted device, including 5/8 subjects in GCC countries, and 32% did not have a device password. Further, 57% of subjects did not have a contingency plan if they lost their device.

3.5.1 Use of phones

We examined 28 phones, one per subject, except for two subjects (both from (D)) who had time constraints (Table 5).

Table 5. Phones we examined

	(H)	(G)	(D)	(M)	Total
Android	3/4	3/8	4/6	8/10	18/28
iOS	0/4	5/8	2/6	2/10	9/28
BlackBerry	1/4	0/8	0/6	0/10	1/28

Multiple Phones: The four members of (H) used BlackBerry phones for their organizational/work email account. Three of them used other phones as well, including for work-related activities. For the subject that exclusively used a BlackBerry, we examined their BlackBerry. In the other cases, we examined their other phones. Three other subjects reported using multiple phones, including one who used two iPhones with different mobile providers, because one had better coverage at his house, and one had better coverage at his office; one who used both iPhone and Android; and one who used three different Android phones. We asked to examine these subjects' primary phone.

One subject (S_{12}) also used several triple-SIM phones that were not smartphones, in order to prevent calls he made to different individuals (using different SIMs) from being linked together by governments in countries where he works. He

stated that he has a multitude of SIM cards, and uses certain SIM cards only to talk to certain people, in some cases only calling a single contact from a SIM card. He also stated that he swaps SIM cards frequently as he travels. (We explained that each SIM slot is also uniquely identified with an IMEI, and thus if he swapped the SIM cards around to different slots, this would be one way his SIM cards could be linked together.)

3.5.2 Updates

We measured how many days out-of-date a subject's phone's operating system was by taking the difference between the release date of its OS version, and the release date of the latest version available as of the interview date. Out-of-date phone OS versions can be used to target victims. For instance, Hacking Team had a zero-day exploit for the default web browser in older Android versions 4.0-4.3 [25]. Hacking Team also used several known exploits to *root* older versions of the Android OS, including CVE-2012-6422, CVE-2013-6282, and CVE-2014-3153 [25, 26].

One of the nine iPhones we examined was out-of-date (43 days); the rest of the iPhones were up to date. We plot the results for the 18 Android phones we examined in Figure 2.

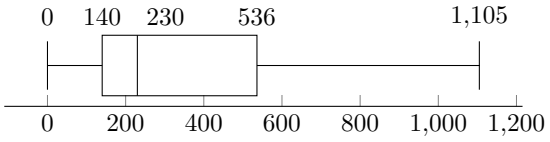

Fig. 2. Days out-of-date (Android OS version). Horizontal box plot showing quartiles.

3.5.3 Security Settings

We checked a variety of security settings on subjects' phones (Table 6).

Table 6. Phone security settings

	(H)	(G)	(D)	(M)	Total
Unencrypted	3/4	5/8	3/6	8/10	19/28
WAP Push	3/4	3/8	3/6	6/10	15/28
Sideloading	1/4	2/8	1/6	2/10	6/28
Rooted	0/4	2/8	0/6	0/10	2/28

Rooting is the process of gaining administrator-level privileges on a device; on an iPhone, *jailbreaking* includes rooting, as well as circumventing other iPhone security measures. We marked a phone **Rooted** if it was a rooted Android phone or a jailbroken iPhone.

One subject (S_8) from (G) jailbroke his iPhone in order to install a second copy of WhatsApp to use with an overseas phone number not linked to his name (to remain anonymous when communicating with certain people). A second individual from (G) (S_{14}) rooted his Android in order to install *X Privacy*, an app that enables fine-grained permissions control over Android apps. Rooting and jailbreaking can be a security risk; both FinFisher and Hacking Team require rooting or jailbreak for all mobile spyware features to be available [27, 28].

Sideloading is the process of installing apps from outside of the phone's app store. Any Android user can enable sideloading in the phone's security settings.[11] The iPhone does not have such an option, but jailbreaking allows sideloading. We counted the number of phones that had sideloading enabled as of interview time. S_{27} from (H) enabled sideloading to install Grooveshark, a (now former) music streaming service of undetermined legality. S_{10} from (D) enabled sideloading to install Aptoide (an alternative app store), and S_{20} from (G) enabled sideloading to install Popcorn Time (a P2P Netflix clone). Two individuals from (M) (S_3, S_{23}) were unsure as to why sideloading was enabled on their phones.

One subject (S_{11}), who did not have sideloading enabled on their current phone, remarked about their past usage of the feature: *"[I installed] an app transfer software. I wanted to transfer one of these apps to my friend. A friend in* [HoA Country] *gave me an APK for the app transfer software, to transfer apps through Bluetooth. The Internet in* [HoA Country] *is so slow, really hard to get a connection."*

Enabling sideloading can be a security risk, as this allows the installation of apps that have not been vetted by the app store. One attack apparently asked dissidents to install an APK file from a link [26]. Sideloading can pose an additional concern in concert with **WAP Push** *service* messages. WAP Push messages are SMS messages that may be presented to the user by the phone in a way that makes them appear to originate from the user's mobile phone carrier. WAP *Service Indication (SI)* messages may contain text and a link. Hacking Team and FinFisher documentation suggest that this technique may be used to send targets links to fake updates [29, 30]. WAP *Service Loading (SL)* messages may try to execute an action on a recipient's phone, such as installing an app from a file on a website. As far as we are aware, WAP Push service messages are not supported on iPhones. Fifteen Android phones had WAP Push messages enabled, while requiring a prompt

11 When attempting to install an APK file on an Android where sideloading is disabled, the user receives an "Install Blocked" message, with a link to the Android settings page where the user may enable sideloading.

before any action associated with an SL message is taken (the default). Five Android phones did not have any WAP Push message options, and we assumed these did not support WAP Push messages.

We consider iOS versions from 8 onward to be encrypted [31], as well as any Android that has the encryption option enabled.[12] Other phones are marked **Unencrypted**.

One subject whose phone appeared to be encrypted (according to Android settings) complained that they had enabled encryption, but at some point their device stopped prompting them for a password when it booted. Therefore they were unsure as to whether their phone was still encrypted.[13]

One subject whose phone was not encrypted (S_{29} from (G)) mentioned that they wanted to use a pattern password with encryption, but were unable to do this, and that having a password they had to type out was *"too inconvenient."* The same subject was also concerned about the auto-wipe feature. He mentioned a previous occasion on which he set up encryption and enabled auto-wipe, which was set to wipe his phone after five incorrect passwords. The subject was subsequently arrested; police confiscated his phone and input five incorrect passwords, and he lost all of the data on his phone. Another subject (S_9 from (G)) whose phone was not encrypted mentioned that the instructions were too complex, and believed that if he enabled encryption, he could only exchange files with people who had the same version of Android.

We checked what type of password was enabled on each phone (Table 7).

Table 7. Phone password settings

	(H)	(G)	(D)	(M)	Total
No password	1/4	2/8	1/6	5/10	9/28
Pattern	2/4	2/8	2/6	2/10	8/28
4 digit	1/4	3/8	2/6	1/10	7/28
6 digit	0/4	0/8	0/6	2/10	2/28
Alphanumeric	0/4	1/8	1/6	0/10	2/28

A **Pattern** password (Android) allows a user to unlock their phone by connecting dots on a 3x3 grid. There are 389,112 possible pattern passwords [32].

3.5.4 Lost Phone

We asked subjects what they would do if they *"lost or misplaced"* their phone (Table 8).

Table 8. Subjects' action if phone "lost or misplaced"

	(H)	(G)	(D)	(M)	Total
No strategy	2/4	4/8	5/8	8/10	17/30
Trace phone	0/4	2/8	2/8	1/10	5/30
Wipe phone	0/4	1/8	0/8	0/10	1/30
Use backup	0/4	1/8	1/8	1/8	3/30
Other	2/4[14]	1/8[15]	1/8[16]	1/10[17]	5/30

We classified subjects into the **No strategy** category if they had a response similar to *"nothing," "I don't know,"* or *"pray"* (S_{29}). Of the subjects who had no strategy, one subject from (G) (S_7) said they were aware of the option to remotely wipe their phone, but thought it was too complicated to set up. One subject from (D) (S_{10}) said they formerly used a remote wipe program, but did not set it up on their current phone. One subject from (M) (S_{23}) had a *"vague recollection"* of setting up software to track their phone if it was lost, but had no idea how to use it. Another subject from (M) (S_{22}) said *"I never think about these questions."* One subject from (M) (S_{26}) remarked only: *"I am supposed to back up everything on the cloud, which I have not"* in response to the question.

3.5.5 Security apps

We asked subjects if they used any security or privacy apps on their phones (Table 9).

Table 9. "Security or privacy apps" mentioned by subjects

	(H)	(G)	(D)	(M)	Total
Antivirus	0/4	2/8	2/8	2/10	6/30
Secure chat	0/4	2/8	2/8	0/10	4/30
App lock	0/4	1/8	1/8	0/10	2/30
Other	0/4	4/8[18]	2/8[19]	0/10	4/30

12 We interviewed one individual in May 2014, who was using iOS 7.1.1 (the latest at the time). We counted his phone as unencrypted.

13 We still counted this phone as encrypted, because the option for encryption was enabled.

14 Two subjects said they would contact their IT department.

15 One subject said they would change their passwords.

16 One subject said they would call the police.

17 One subject said they would call their phone manufacturer or telecom company.

18 Subject S_{14} mentioned using APG with K-9 Mail, X Privacy, Avast Anti-Theft, SyncThing, and Ccleaner. Subject S_{15} mentioned *unfurlr*, and *Video Downloader Pro*, which they employed to "lock files with a PIN code." Subject S_8 mentioned their use of VPN.

The **Antivirus** apps used by subjects included *Avast*, *Avira*, *Clean Master*, *Lookout*, *Malwarebytes*, and *McAfee*. One subject, S_{21}, was using three different antivirus apps at the same time, and the five other current users of **Antivirus** apps used a single app. Several subjects noted issues with antivirus apps. Subject S_{21} remarked that they formerly used messaging app Telegram, but uninstalled it because Malwarebytes indicated it was malicious. Subject S_5, a McAfee user, expressed their annoyance at how the app would bother them with *"frequent messages and promotions."* Former antivirus app users also noted issues that caused them to stop using such apps. Subject S_{11} said they formerly used *AVG* antivirus on their phone, but uninstalled it because they said they *"don't usually use"* it, and wanted to free up space. Subject S_{23} said they formerly used Avast, but uninstalled it because *"there were too many notifications, it killed most of the activities of my phone, it appeared to be a virus."*

Four subjects cited their use of **Secure chat** apps. S_2 cited *Chatsecure*, S_{15} and S_{21} cited *SureSpot*, and S_{25} cited their use of *Signal*.

Two subjects, S_2 and S_{21}, reported using an app that allowed them to "password protect" other apps (**App lock**). Both subjects used Clean Master for this purpose.

We asked Android subjects: *"Have you ever declined to install an app based on the permissions it requested?"* and iPhone subjects *"Have you ever declined a permission request for an app?"* (Table 10). One subject was unsure, four subjects reported that they did not install apps (**Don't install**).

Ten subjects provided additional detail about under what circumstances they declined permissions requests. Subjects cited **Updates** that requested additional permissions, access to their **Location** or **Contacts**, or whether they felt the request was **Unreasonable**. There was no overlap between responses.

Table 10. Declined permissions requests or app installs

	(H)	(G)	(D)	(M)	Total
Yes	2/4[20]	8/8	6/8	3/10	19/30
No	0/4	0/8	1/8	5/10	7/30
Don't install	2/4	0/8	0/8	2/10	4/30
What is declined					
Location	0/4	2/8	1/8	1/10	4/30
Unreasonable	0/4	2/8	0/8	1/10	3/30
Updates	1/4	0/8	1/8	0/10	2/30
Contacts	0/4	0/8	1/8	0/10	1/30

Of the subjects who did not decline permissions, S_3 remarked that they *"don't read any of the permissions, just click the agreement and go for it,"* but added that they *"don't use a lot of apps."* Subject S_{11} remarked that they *"thought Play store was trusted, so didn't really think about declining because of permissions."* Subject S_6 (an Android user) said they did not decline installation due to permissions, but remarked that they sometimes did not use an app after install if the app prompted them to enter their password, or credit card details.

3.6 Internet Browsing

We asked respondents if they used Tor or a VPN. These tools can be useful for preventing government deanonymization of online accounts, and can additionally help avoid local government tracking of visited websites and interception of sensitive plaintext data via passive surveillance, as well as local government *network injection*. Subject responses also revealed some pitfalls of security tools.

Table 11. Subject use of VPNs and Tor

	(H)	(G)	(D)	(M)	Total
VPN phone	0/4	5/8	1/8	0/10	6/30
VPN PC	0/4	2/8	1/8	0/10	3/30
Tor PC	0/4	3/8	0/8	1/10	4/30
Total	0/4	6/8	1/8	1/10	8/30

One subject from (D) (S_{21}) and one subject from (G) (S_{14}) reported using a VPN all the time on their computer and phone. One subject from (G) (S_8) reported using two different VPNs; they had heard that one was *"more secure,"* and one functioned better with *"slow Internet speeds."* Subject S_8 used the VPNs to post to a pseudonymous online account. One subject from (G) (S_{15}) said they used a (different) VPN on their computer and phone if they felt what they were doing was *"sensitive."* One subject from (G) (S_9) said they used a VPN on their phone when they *"suspect something is being checked or monitored, or to get around censorship."* One subject from (G) (S_{20}) said they used a VPN on their phone to watch Western TV shows.

Two subjects from (G) (S_2, S_7) said they used to use a VPN; S_2 said they switched to Tor browser, and S_7 said they found VPN usage to be too complicated.

Subject S_8, who was concerned about interception of their passwords, requested that we test to see whether their passwords were being transmitted in plaintext from their phone. We connected the subject's phone to the Internet via our laptop, and observed their Internet traffic for a brief period. We were able to capture a password for one of their pseudony-

19 Subject S_{10} mentioned "Samsung Security Policy Update." Subject S_{21} mentioned their use of VPN.

20 S_{27} remarked that they used to decline permissions, but do not do so anymore.

mous accounts on a blogging site. They were using a blogging app on their phone which transmitted the password in plaintext whenever the app was opened. They had been told to make sure to use the VPN whenever *posting* to a blog, so they first opened the app, and then connected to the VPN before submitting a post. We advised S_8 to connect to the VPN before opening the blogging app.

We examined two computers (both from (G)) that had Tor Browser installed. Both copies of Tor Browser were out-of-date. Subject S_2 exclusively accessed their email account through Tor. This subject (using Ubuntu) said their Tor browser was out-of-date because on one previous occasion, installing updates had rendered their Tor browser unusable. Therefore, S_2 was not updating their Tor browser, or their Ubuntu system (they had 600+ updates pending in Ubuntu).

We helped the subject get their system up to date and ensure that Tor browser continued to work. The other Tor subject, S_{15}, said they used Tor only occasionally for *"sensitive"* things. One subject from (G) (S_{14}) and one from (M) (S_{26}) said they used Tor rarely or occasionally; we did not find Tor Browser on the computers of theirs that we examined.

Five subjects claimed to be former Tor users. Subject S_4 from (M) stated that they had tried it once, but *"sometimes it won't let you go to certain pages."* Subject S_{19} from (M) stated that they *"learned about it at the training...but don't use it anymore."* Subject S_{11} from (M) stated that *"somehow, it crashed 2 or 3 times so I uninstalled it."* Subject S_{21} from (D) stated that they *"used to, but I mean generally, it slows down everything so I stopped using it a few years ago."* Subject S_7 from (G) said they tried to use Tor, but found it too complex. They said that solutions like Tor *"aren't catered to part-time activists, only for hardcore activists that do it all the time."*

We classified 12 subjects into the **No strategy** category, because they remarked that they did not know (9 subjects), their recovery account information was out-of-date (2 subjects), or they indicated they would do nothing (S_{23} from (M) indicated they would leave their old accounts *"for dead"* and create new accounts). Sixteen subjects believed they had up to date **Recovery account** information (either a recovery email account or recovery phone or both).

Two subjects mentioned **Other** methods of recovery. One subject from (G), who was part of an organized activist group that was the subject of recent arrests, remarked that their organization used a person outside of the country as a *"password manager."* That person had access to all of the passwords used by the various groups, and could recover accounts or change passwords if necessary. One subject (S_7) remarked that if they lost access to their accounts, they would reach out to friends at Facebook and Twitter to recover access.

We asked respondents how likely (on a scale from 1-5) they thought it was that governments would try to take the passwords of arrested activists (Figure 3), and use accounts of arrested activists to target friends (Figure 4). This question was motivated by previous work that found accounts of arrested activists employed to successfully target their friends [2].

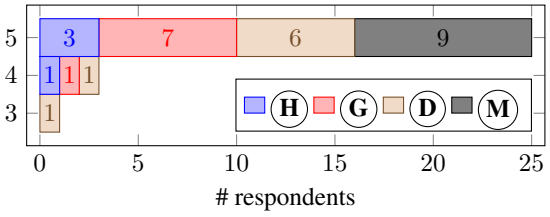

Fig. 3. "How likely is it that the government will steal ... passwords from an activist's phone or computer when they are arrested?" (1: definitely not; 5: definitely)

3.7 Security of Online Accounts

We asked subjects how they would recover their email and social media accounts if they lost access (Table 12). Losing account access may be a symptom of phishing or device compromise; if an attacker takes over a victim's account, they may use it to target the victim's friends and contacts. We also asked for subject perspectives on whether governments would seek to use accounts of imprisoned dissidents in this fashion: 73% of subjects viewed this as a certainty.

Table 12. Subjects' action if they lose access to online account

	(H)	(G)	(D)	(M)	Total
Recovery account	0/4	6/8	3/8	7/10	16/30
No strategy	4/4	0/8	5/8	3/10	12/30
Other	0/4	2/8	0/8	0/10	2/30

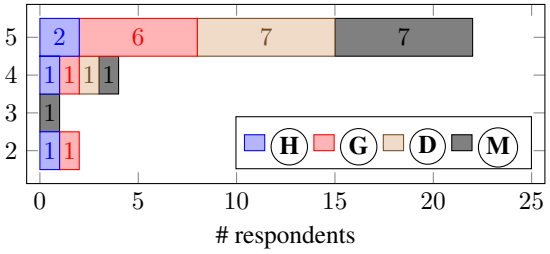

Fig. 4. "How likely is it that the government will use arrested activists' ... accounts to target their acquaintances?" (1: definitely not; 5: definitely)

3.8 Checking links and attachments

Malicious links and attachments are a common vector for social engineering attacks on dissidents. While most subjects reported that they vet such messages, and perceive reduced risks from interacting with the message afterwards, the methods they use appear to be vulnerable to social engineering.

3.8.1 Message vetting techniques

We asked subjects about how they checked messages containing links and attachments that they receive: *"Do you check links before opening them to see if they are safe? How?"* (and repeated for attachments). The results for links and attachments were broadly similar, except two subjects (both from (D)) reported checking links but not attachments. We record how subjects checked links and/or attachments in Table 13. Five subjects reported that they did not check either links or attachments.

Table 13. How do subjects check links or attachments?

	(H)	(G)	(D)	(M)	Total
Sender	3/4	5/8	3/8	10/10	21/30
Context	3/4	4/8	0/8	4/10	11/30
2nd Factor	2/4	0/8	0/8	4/10	6/30
Tools	0/4	2/8	1/8	0/10	3/30
Gmail	0/4	2/8	2/8	2/10	6/30
Other	2/4[21]	1/8[22]	0/8	1/10[23]	4/30
Total	3/4	7/8	5/8	10/10	25/30

Some subjects reported checking the **Sender** of the message; some checked the **Context** surrounding the message (e.g., if the message was *"out of the ordinary"* for the sender, whether it was *"generally addressed,"* whether the sender properly greeted the recipient); some made use of a **2nd Factor**, e.g., placing a phone call to the purported sender, to ask if they had sent the message; some subjects used **Tools** to check links and attachments themselves, such as VirusTotal, their computer's antivirus (before opening an attachment), or various websites to unshorten URLs; and some relied on **Gmail** warnings, or used the preview feature in Gmail to check the attachment before they downloaded it.

When prompted about their checking of links and attachments, three subjects from (M) mentioned that sometimes their computers run slow after opening a link or attachment, and this leads them to be suspicious about surveillance (S_6, S_{11}, and S_{23}).

Two subjects from (M) articulated a feeling that they were safe using Gmail: S_{19} stated: *"Experts say Gmail is safe,"* and subject S_{26} said: *"Gmail always gives you a sign if something's wrong. They have some kind of notification system that this may contain a virus."*

Subject S_{26} also remarked that he could tell if a message was malicious: *"when you experience a lot of being victimized and targeted, you develop intuition and are cautious about these things."* A few weeks after the interview, the subject forwarded a message to the authors that he thought was suspicious. He remarked that he had downloaded and opened the attachment on his computer, and only later realized that the sender account was crafted to look like one of his friends, but did not actually belong to the friend. The attachment did not contain spyware, but a link in the email led to a website that contained spyware. The subject had not interacted with the website sufficiently to infect his computer.

3.8.2 Subject perception of vetting efficacy

We asked subjects to rate the safety of opening links and attachments before and after they had checked them. We show the results for attachments in Figure 5. We excluded five subjects who did not check attachments, and four subjects who answered *"don't know."* The results for links paint a similar picture.

3.9 Take-aways

Overall, most respondents seemed concerned with ensuring the privacy of information on their computers, phones, and online accounts, or consequences stemming from the compromise of private information.

3.9.1 Optional vs mandatory security

A significant number of subjects did not enable optional security features on their devices or online accounts; only 68% of phones had a password of some type; 53% of subjects had a strategy for recovering access to an online account if they lost access; 44% of subjects had a strategy for recovering from loss of a mobile device; and 32% of phones were encrypted. Focusing on making such features mandatory while causing

21 Hovers over links.

22 One mentioned checking extensions on links, and not clicking on shortened links.

23 One mentioned checking the URL of links, and extensions on attachments.

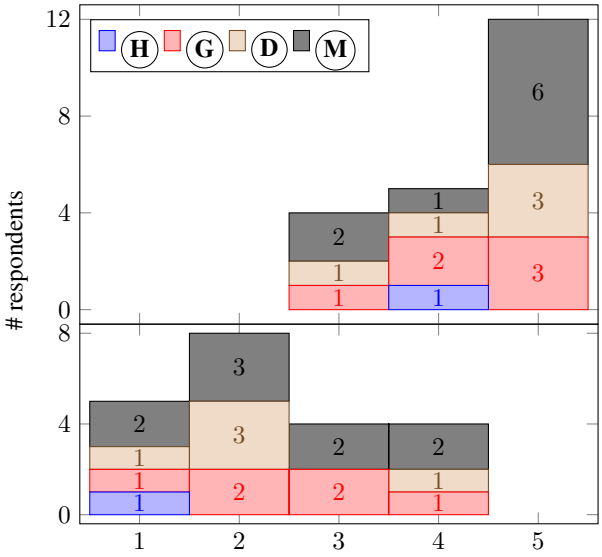

Fig. 5. Subjects' perceived risk of opening attachments before (top) and after (bottom) "checking." (1: completely safe; 5: not at all safe)

minimal inconvenience for users could help ease these security concerns.

3.9.2 Folk models and ad hoc defenses

Several subjects appear to use *ad hoc defensive strategies* for responding to perceived security risks. For instance, two subjects (S_2 and S_{21}) reported using app lock software, and one (S_{15}) reported using file lock software. It is an open question how effective such apps are; Trend Micro found vulnerabilities in some app locking products it analyzed [33].

In some cases, these strategies may introduce new security vulnerabilities. For instance, the subject's (S_{12}) use of triple-SIM phones and frequent SIM swapping to prevent linkage of communications with different contacts (Section 3.5.1) could introduce issues if the same SIM card is ever used in more than one slot. The subject's (S_8) jailbreaking of their iPhone to install a second copy of WhatsApp with a number not registered in their name may help preserve anonymity of WhatsApp communications, but could increase risks from spyware. Similarly, the subject's (S_{14}) rooting of their Android to install *X Privacy* may help the subject better control information shared by their apps, but could increase spyware risks.

We also identified the possible presence of security *folk models*: mental models that are not necessarily correct, and may lead to suboptimal security decision making [34]. For instance, S_{11}'s statement that the "[Google] Play store [is] trusted" leading them to not check permissions of apps they install, S_{10}'s belief that "Gmail is safe," and S_{26}'s belief that "Gmail always gives you a sign if something's wrong." Three subjects believed that computers running slow was a possible sign of surveillance (S_6, S_{11}, and S_{23}).

3.9.3 Vulnerability to social engineering

Broadly, subjects appear to be vulnerable to social engineering along several different dimensions.

Subjects' methods for checking links and attachments (primarily checking sender addresses and vetting a message's context) would seem to be vulnerable to more advanced social engineering. Indeed, one subject, S_{26}, who indicated that they checked a message's sender address and context, opened an attachment from an account designed to impersonate a friend (Section 3.8).

Deficiencies in subject security settings, physical security, as well as in contingency plans for recovering from account and phone loss, could lead compromised accounts to be used in social engineering, as has been documented in previous work [2].

Further, some subjects expressed a desire to focus on their work, or a frustration with digital security. As S_{19} from (M) put it *"Life is intense, you focus on your work. People ... are suffering and in prison, when you focus on that you forget yourself."* Subject S_{27} from (H) wondered *"Should I spend half a day figuring out digital security, or do work?"* Subject S_7 from (G) stated *"you have to open attachments. you can't allow yourself to be a permanent victim of malicious intent. life has to move on."*

4 Conclusions and Future Work

Our survey of potential targets of abusive government attacks finds they have numerous vulnerabilities to new methods of dissident surveillance that involve social engineering. Despite the availability of free online tools to check links and attachments, our subject population does not appear to widely use such resources.

Our results suggest that a tool supporting *automatic checking* of email messages may provide some benefit to our study population. As previous work [1–3] has shown, many attack campaigns targeting this population employ similar techniques (e.g., Microsoft Office documents that try to run executable files, IP logging links). A defensive tool could look for certain behavioral signatures that are more likely to be malicious in the context of potentially targeted users than in an ordinary population (e.g., IP logging links), as well as conducting scans against indicators (e.g., [35]) known to be part

of targeted attacks. Depending on subjects' preferences, scanning could go beyond the traditional scanning provided by email services, by attempting to unshorten and download certain links included in emails to check their contents. We have currently obtained IRB approval for, and are developing and evaluating, such a scanning tool.

References

[1] S. L. Blond, A. Uritesc, C. Gilbert, Z. L. Chua, P. Saxena, and E. Kirda, "A Look at Targeted Attacks Through the Lense of an NGO," in *23rd USENIX Security Symposium (USENIX Security 14)*, Aug. 2014.

[2] W. R. Marczak, J. Scott-Railton, M. Marquis-Boire, and V. Paxson, "When Governments Hack Opponents: A Look at Actors and Technology," in *23rd USENIX Security Symposium (USENIX Security 14)*, Aug. 2014.

[3] S. Hardy, M. Crete-Nishihata, K. Kleemola, A. Senft, B. Sonne, G. Wiseman, P. Gill, and R. J. Deibert, "Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware," in *23rd USENIX Security Symposium (USENIX Security 14)*, Aug. 2014.

[4] "FinFisher - Excellence in IT Investigation," accessed: 27-February-2014. [Online]. Available: http://www.finfisher.com/

[5] "Hacking Team," accessed: 27-February-2014. [Online]. Available: http://www.hackingteam.it/

[6] N. Group. [Online]. Available: https://web.archive.org/web/20120813064018/http://www.sibat.mod.gov.il/NR/rdonlyres/DADE8D1E-DFAA-4143-BB48-A73C77C88CBA/0/NSOGROUPE.pdf

[7] J. Cox, "A Hacker Claims to Have Leaked 40GB of Docs on Government Spy Tool FinFisher," Aug. 2014. [Online]. Available: http://motherboard.vice.com/read/a-hacker-claims-to-have-leaked-40gb-of-docs-on-government-spy-tool-finfisher

[8] A. Greenberg, "Hacking Team Breach Shows a Global Spying Firm Run Amok," Jul. 2015. [Online]. Available: https://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/

[9] FinFisher, "Remote Monitoring & Infection Solutions: FinFly ISP," Spy Files, 2011, accessed: 30-August-2016. [Online]. Available: https://wikileaks.org/spyfiles/files/0/297_GAMMA-201110-FinFly_ISP.pdf

[10] Hacking Team, "Hacking Team: Network Injector Appliance," Hacking Team email dump, 2015, accessed: 30-August-2016. [Online]. Available: https://wikileaks.org/hackingteam/emails/fileid/447727/212805

[11] J. Scott-Railton and K. Kleemola, "London Calling: Two-Factor Authentication Phishing From Iran," Aug. 2015, accessed: 23-May-2016. [Online]. Available: https://citizenlab.org/2015/08/iran_two_factor_phishing/

[12] Tibet Action Institute, "Detach From Attachments!" Dec. 2011, accessed: 23-May-2016. [Online]. Available: https://vimeo.com/32992617

[13] K. Kleemola, M. Crete-Nishihata, and J. Scott-Railton, "Targeted Attacks against Tibetan and Hong Kong Groups Exploiting CVE-2014-4114," Jun. 2015, accessed: 23-May-2016. [Online]. Available: https://citizenlab.org/2015/06/targeted-attacks-against-tibetan-and-hong-kong-groups-exploiting-cve-2014-4114/

[14] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner, "Investigating the Computer Security Practices and Needs of Journalists," in *24th USENIX Security Symposium (USENIX Security 15)*, Washington, D.C., Aug. 2015.

[15] A. Forget, S. Pearman, J. Thomas, A. Acquisiti, N. Christin, L. Faith Cranor, and S. Egelman, ""My Daughter Fixes All My Mistakes": A Qualitative Study on User Engagement and Computer Security Outcomes," in *SOUPS*, 2016.

[16] "AOL/NCSA Online Safety Study," Oct. 2004. [Online]. Available: https://web.archive.org/web/20051102045804/http://www.staysafeonline.info/pdf/safety_study_v04.pdf

[17] "Media Use in the Middle East," 2015, accessed: 30-November-2016. [Online]. Available: http://www.mideastmedia.org/survey/2015/

[18] H. Choi, B. B. Zhu, and H. Lee, "Detecting malicious web links and identifying their attack types." USENIX Conference on Web Application Development 2011, 2011. [Online]. Available: http://research.microsoft.com/apps/pubs/default.aspx?id=193308

[19] S. Afroz and R. Greenstadt, "Phishzoo: Detecting phishing websites by looking at them," in *Fifth IEEE International Conference on Semantic Computing (ICSC)*. IEEE, 2011, pp. 368–375.

[20] "Reflecting on Ten Years of Practice: The Challenges of Digital Security Training for Human Rights Defenders." Tactical Technology Collective, accessed: 30-August-2016. [Online]. Available: https://secresearch.tacticaltech.org/reflecting-on-ten-years-of-work-the-challenges-of-digital-security-training-for-human-rights-defenders

[21] "National Endowment for Democracy," accessed: 30-November-2016. [Online]. Available: http://www.ned.org/

[22] "Front Line Defenders," accessed: 30-November-2016. [Online]. Available: https://www.frontlinedefenders.org/

[23] "Internews," accessed: 30-November-2016. [Online]. Available: https://www.internews.org/

[24] F. Lalonde Levesque, J. Nsiempba, J. M. Fernandez, S. Chiasson, and A. Somayaji, "A Clinical Study of Risk Factors Related to Malware Infections," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*. New York, NY, USA: ACM, 2013.

[25] A. Marosi, "Hacking Team: how they infected your Android device by 0days." Presented at Hack.lu 2015, 2015. [Online]. Available: http://archive.hack.lu/2015/HT_Android_hack_lu2015_v1.0.pdf

[26] M. Marquis-Boire, J. Scott-Railton, C. Guarnieri, and K. Kleemola, "Police Story: Hacking Team's Government Surveillance Malware," Jun. 2012, accessed: 17-May-2016. [Online]. Available: https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant/

[27] FinFisher, "FinSpy Mobile 4.51–Release Notes," FinFisher document dump, 2014, accessed: 30-August-2016. [Online]. Available: https://netzpolitik.org/wp-upload/Release-Notes-FinSpy-Mobile-4.51.pdf

[28] P. Vinci, "Fwd: PUMA updated Proposal - version 3," Hacking Team email dump, 2015, accessed: 30-August-2016. [Online]. Available: https://wikileaks.org/hackingteam/emails/

emailid/1094866
[29] M. Luppi, “I: I: BULL. RMI addtional questions,” Hacking Team email dump, 2015, accessed: 30-August-2016. [Online]. Available: https://wikileaks.org/hackingteam/emails/emailid/437543
[30] FinFisher, “FinSpy Mobile 4.00 User Manual,” Spy Files 4, 2014, accessed: 30-August-2016. [Online]. Available: https://wikileaks.org/spyfiles4/documents/FinSpyMobile-4.00-User-Manual.docx
[31] Apple, “Government Information Requests,” accessed: 17-May-2016. [Online]. Available: https://www.apple.com/privacy/government-information-requests/
[32] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, “Smudge Attacks on Smartphone Touch Screens,” in *ACM CCS*, 2009, pp. 512–523.
[33] S. Huang, “The Severe Flaw Found in Certain File Locker Apps,” 2014, accessed: 30-August-2016. [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/the-severe-flaw-found-in-certain-file-locker-apps/
[34] R. Wash, “Folk Models of Home Computer Security,” in *SOUPS*, Jul. 2010.
[35] Citizen Lab, “Malware Signatures,” GitHub repository. [Online]. Available: https://github.com/citizenlab/malware-signatures