access

GLOBAL CIVIL SOCIETY AT RISK:

AN OVERVIEW OF SOME OF THE MAJOR CYBER THREATS FACING CIVIL SOCIETY

January 2012

/// /// GLOBAL CIVIL SOCIETY ////// /// AT RISK: /////////////////////////////////

///AN OVERVIEW OF SOME OF THE MAJOR ////////// ///CYBER THREATS FACING CIVIL SOCIETY ///////////// //

For more information, please contact:
soc@accessnow.org
PGP Key ID: 0xF08D380A

NOTE: This brief aims to detail the major threats faced by global civil society in 2011. It is based on our experiences over the past year and reports on incidents faced by people in our wider community. While it cites empirical data, this report should not be read as a complete catalog of incidents internationally. Data, evidence of other attacks and comments are welcomed and should be directed to ***soc@accessnow.org (PGP Key ID: 0xF08D380A)***

INTRODUCTION

As it becomes increasingly important for civil society movements and activists to be able to consistently operate freely, fully, and safely online, they have found themselves at a high level of risk from cyber attacks. The internet has proven to be one of the most important factors in the efficacy of social change and evolution in the 21st century. In recent years, civil society has had some success in achieving its goals across the globe, and the opponents of social change are well aware of this. These opponents, including the authoritarian regimes of closed and semi-closed societies, have also shown they will not hesitate to quash or manipulate the communication of a nation's citizenry in order to suppress participation and to retain their grip on power. Indeed, the front line of cyber warfare is often being fought by regimes and governments against civil society, but this fight isn't only about political repression; LGBT activists, environmental advocates, and corporate campaigners are facing similar foes, who are using the internet to disable, disarm, and neuter them.

The wide range of opponents to the diverse makeup of global civil society have put a great amount of energy and resources into increasing their capability in cyber warfare and placing themselves on the cutting edge of offensive cyber warfare technology. Unfortunately, the same cannot be said for many activists nor the NGO's that support and assist them.

Deep information security knowledge, skills, and experience are often in short supply within civil society, and this leads to both a lack of awareness of the problems as well as a dearth of high-tech security training that is required by individuals operating within civil society movements. This situation can lead to significant security breaches. All too often NGO staff and activists realize how serious the situation is when communications with a colleague suddenly cease and their fate becomes unknown. Such a situation can highlight the difficulty of operating in hostile environments where it only takes one link in the chain to use insecure processes to compromise the whole chain.

It is imperative that members of the global technology community, including the corporate sector, consider what they can do to assist civil society to meet the cyber threats they face. This may be building human rights into their products by design. It may be by scaling pricing structures for products so that NGOs are able to obtain the same level of cyber defense capability given their often limited budgets. It may be sharing of cyber intelligence with civil society. It may come through contributing technology to the open source community. Whatever form it takes, there is no question that civil society is under threat and requires partnerships and assistance. It also places the imperative on governments which are in a position to fund, secure and establish new norms that deliver better security to civil society. In turn, the experience gained by civil society, arising from the cyber attacks being conducted against them, may provide value to the broader community in the form of helping all of us better prepare for new cyber threats that have not yet filtered down into the hands of organized cyber criminals or other actors.

//

IDENTIFIED THREATS

Since Access (www.accessnow.org) was founded in the wake of the 2009 Iranian post-election crackdown, we have witnessed many cyber attacks upon on-the-ground contacts, partner organizations, and other members of civil society around the world. From our experience, we have compiled the following list of threats that we believe are at present amongst the most significant faced by civil society. We look forward to working with others in the sector and beyond to compile additional data that can be historically framed and appropriately categorized in order to get a clearer picture in 2012 of the scale of the problems outlined here.

DENIAL OF SERVICE (DoS) ATTACKS

Denial-of-service attacks are attacks designed to make a particular site or service inaccessible. Typically, this is accomplished by sending massive amounts of traffic to the site which, as it struggles to handle all the incoming requests, becomes overloaded and either crashes or becomes too backlogged to respond. A real-world analogue might be dumping 500 tons of potatoes in front of a shop door, preventing anyone from walking into the shop. A variant of DoS attacks, known as DDoS, for distributed denial-of-service, is a DoS attack in which the mass of traffic comes from thousands or even millions (in some cases) of different sources. The effect is the same, but a single-source DoS attack can be stopped by blocking that single source. A DDoS attack cannot be so simply shut off, as it would require blocking large, unpredictable portions of the net. DDoS attacks, also like spam, typically rely on myriad virus-infected computers that get their orders from a command-and-control server elsewhere that forms them into a botnet — the attacking traffic comes from, effectively, innocent bystanders.

These attacks are difficult to trace back to their perpetrators or the parties in power who may have ordered them, but increasingly DoS is being used as a tactic to silence opposition voices. DoS attacks are particularly effective where information is time-sensitive, such as in the lead-up to elections. These attacks do not permanently damage the target sites, but the disruptive effect is clear. DoS capability can be hired from established cyber criminals, who provide all the technical support you'd expect from a commercial vendor.

In a December 2011 report on Russia, Agora Human Rights Association found 25 attacks on federal and regional sites on election days and the days just before them.[1] These included federal and regional sites and electoral commissions with a combined audience of 7 million. In April 2011, Chinese hackers attacked the US site Change.org after that site hosted an online petition calling for the release of the Chinese artist Ai Weiwei.[2, 3]

Also in April 2011, the opposition site Sarawakreport.org was DDoSed, apparently by the Malaysian government.[4] In July 2011, the Malaysiakini news servers successfully withstood a DoS attack (the site had hardened its servers after a previous, similar attack), though its subscription service was affected.[5]

Governments are not the only source of such attacks; any group with an agenda can decide to use this tactic. On November 11, 2011 the so-called hacktivist "Anonymous" group launched DDoS attacks on the websites of the opposition party The Muslim Brotherhood, taking the sites down for at least 6 hours.

BLOCKING AND FILTERING

Despite Internet pioneer John Gilmore's encomium, "The Net sees censorship as damage, and routes around it," the restriction of the free flow of information online poses a very real problem for civil society. In this, civil society has allies among the big Internet companies who are also disrupted by censorship. Former Google CEO Eric Schmidt, for example, has consistently opposed all forms of Internet censorship. Many countries would claim to agree that freedom of speech is paramount — and yet almost every nation has some category of information they believe should be restricted, from online gaming to feminism and gay rights.

Some of the world's most democratic nations began developing filtering technology early in the Internet's history with the stated goal of protecting children from being exposed to "inappropriate" material — anything from pornography to hate speech. In 2010 Australia began its second attempt at nationwide filtering; in the UK, recent governments have claimed as a high priority ensuring that all the nation's consumers are covered by filtering (such as British Telecom's Cleanfeed). As of the end of 2011, both the US and UK are considering legal proposals to block certain sites bearing unauthorized copies of copyrighted material on a national level.

What democratic countries do in the interest of guarding corporate interests and children is being copied by other countries for political ends. Many other countries have institutionalized filtering on a local or national level that allows them to block specific websites (such as foreign or independent news sites, sites belonging to opposition parties, social networks, and open search engines) or whole ranges of IP addresses. Most famously, China

[1] http://agora.rightsinrussia.info/reports/cyberattacks

[2] http://www.networkworld.com/news/2011/042011-changeorg-victim-of-ddos-attack.html

[3] http://www.eweek.com/c/a/Security/FBI-to-Investigate-ChinaBased-DDoS-Attacks-Against-Changeorg-587229/

[4] http://malaysiakini.com/news/161599

[5] http://www.malaysiakini.com/news/169343

has a countrywide firewall under government control, but it is not alone: by the beginning of 2011 Turkey was blocking an estimated 10,000 sites including that of English scientist Richard Dawkins (as well as news and social sites).[6] In August, an Argentine judge ordered ISPs to block the sites LeakyMails.com and LeakyMails.blogspot.com, both projects to publish documents exposing corruption. However, in this case, the judge specified the IP address to be blocked, leading Argentinean ISPs to block the over 1 million blogs using Google's Blogger service, which demonstrates that vast potential for overblocking — and thereby limits on user rights — that filtering entails.[7]

Whoever deploys it, filtering software has a common set of problems. Blocking is not always transparent; service providers may or may not tell subscribers that content is being blocked or at whose request. Blocking is often overbroad; filtering software intended to hide sexual content may also block access to sex education or information about breast cancer, or block all of a service provider's sites instead of just the one or two objectionable ones. It can be difficult to tell whether a particular site has been blocked because of objectionable content or as an accidental casualty of a different block — or if a failure to load is simply ordinary Internet "weather." Overall, blocking is a weapon easily turned against any perceived enemy or threat, including civil society.

MAN IN THE MIDDLE (MitM) ATTACKS

In a man-in-the-middle attack the attacker inserts himself — or his technology — in between a user and a target site. Because both parties believe they are dealing directly with each other, the transaction continues as if it were genuine and the man in the middle can harvest information from both sides.

Attacks may have one or more of several goals. The attacker may simply log the details of the transaction in order to pose as the user in the future, enabling them to conduct fraudulent transactions. In the case of a bank account, that future transaction might be transferring money to an account of the attacker's choice; in the case of a protest page it might mean falsifying the information carried on it. Alternatively, the attacker may disrupt the transaction by feeding false information to one or both sides, disrupting communications and trust. In 2011 we saw examples of all of these.

Facebook is a common target because the size of its user base has made it a widely used resource for coordinating protests. In May, the Syrian Telecom Ministry launched a man-in-the-middle attack against secured https access to Facebook. Users saw a "certificate invalid" warning at login, but many clicked past it.[8, 9]

The most significant MitM attacks of 2011, however, were the Comodo (March) and DigiNotar (July) breaches that compromised the entire system of certificate authorities that authenticate cryptographic security for online transactions via SSL.[10, 11] The DigiNotar attack enabled unknown persons in Iran to use a previously issued fraudulent certificate to conduct an MitM attack on Google services in September. An Iranian citizen also claimed to be behind the Comodo hack, which issued fraudulent certificates for Gmail, Hotmail, and Yahoo! mail. The source of these breaches is peculiar, given the incredible reliance on the SSL/CA system by private enterprise, healthcare providers, and financial institutions, and highlights the danger that civil society is under.[12]

SURVEILLANCE

Like filtering technology, surveillance technology got its start in democratic societies and is being exported to others. Britain was already leading the world in CCTV cameras, but after the 9/11 attacks, cameras proliferated in many parts of the US and EU. In March, claiming the need to manage human traffic, China announced it might begin tracking the movements of cellphone users in Beijing.[13]

Other means of surveillance include simply monitoring online content. In June 2011, 63 Bahraini students were expelled from school after using their Facebook accounts to organize pro-democracy protests.[14] In December 2011, South Korea announced it would appoint an eight-person team to examine social media such as Facebook, Twitter, and smartphone applications to locate "harmful or illegal" content.[15]

In 2011, significant work by a number of NGOs revealed the extent to which commercial companies based in open, Western societies such as the US, France, and Britain are profiting by selling communications surveillance technologies to countries where they are being used to perpetrate significant human rights abuses.[16]

These technologies include devices small enough to be carried in a backpack or briefcase that can intercept and decrypt SMS messages and phone calls from all mobile phones within a radius of several hundred meters; software that gives the purchaser complete and undetectable control over a target's computer or mobile phone; and hardware to tap submarine cable landing stations and therefore all communications traffic in and out of countries.

According to Bloomberg's "Wired for Repression" analysis of these documents, in Bahrain torturers have been armed with

[6] http://www.indexoncensorship.org/2011/03/fighting-political-internet-censorship-in-turkey-one-site-won-back-10000-to-go/

[7] https://www.eff.org/deeplinks/2011/08/argentina-isps-ip-overblocking

[8] https://www.eff.org/deeplinks/2011/05/syrian-man-middle-against-facebook

[9] http://www.geekosystem.com/syria-facebook-man-in-the-middle/

[10] http://www.wired.com/threatlevel/2011/03/comodo-compromise/

[11] http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf

[12] http://www.pcworld.com/article/239565/comodo_ceo_says_diginotar_hack_was_statesponsored.html

[13] http://www.theregister.co.uk/2011/03/04/chinese_tracking/

[14] http://www.educationnews.org/international-uk/%E2%80%9Cvindictive-campaign%E2%80%9D-against-teachers-and-students-in-bahrain/

[15] http://www.zdnetasia.com/south-korea-tightens-social-media-monitoring-62303176.htm

[16] http://topics.bloomberg.com/wired-for-repression/

transcripts of text messages and phone conversations obtained using equipment from Siemens and maintained by Nokia Siemens Networks.[17] In Iran, the same facilities are supplied by the UK's Creativity Software and the Irish company AdaptiveMobile Security.[18] The list is long and includes large companies such as Cisco.

After the news broke in November 2011, the Italian company Area SpA pulled out of helping to build an Internet surveillance system in Syria,[19] and the EU's digital agenda commissioner, Neelie Kroes, announced an initiative to encourage technology firms to abandon the practice.[20] Elsewhere, companies such as the Virginia-based TeleStrategies (host of the Intelligence Support Systems conferences, the "trade show" of the surveillance/censorship industry) reacted by defending their efforts, claiming "that's just not my job to determine who's a bad country and who's a good country."[21] Others, like California-based NetApp, claimed to have no knowledge of how those governments obtained their technology (in NetApp's case, a $4 million component of an Internet surveillance system sold to Syria).[22]

Although this trade seems likely to become more regulated in the near future by legislation in the works in the US and EU, the already installed base of these technologies will be in place for a long time to come, with worrying effects on civil society actors in these countries.

COMMUNICATION BLACKOUTS

"Buy ten backhoes," quipped the respected Internet security experts Matt Blaze and Steve Bellovin in 1998, when asked how to take down the Internet. Experience in 2011 showed that earth-moving machinery is hardly necessary, although it can help: in April, an elderly woman scavenging for copper in the woods damaged a couple of cables, taking the country of Armenia offline for 28 hours.[23]

In 2007, Myanmar became the first country to shut down Internet access entirely during a period of violent protests.[24] In 2011, during the "Arab spring" uprisings, the government of Egypt disconnected the country from the Internet entirely for five days.[25] Although Egypt is an important crossing point for underwater cables, only half a dozen companies control almost all citizen Internet access in the country, and efforts were taken to ensure that only Egyptians and not the global internet infrastructure were effected by the blackout. In May, Iran planned to disconnect the country from the worldwide Internet, replacing it with a nationally controlled internal network, the so called "Halal Internet."[26]

In 2011, internet shutdowns were also seen in other "Arab spring" countries, including Tunisia, Libya, Syria, Yemen, and Bahrain.

Other forms of communications have also been subject to deliberate blackout. Broadcast radio and television stations have had their operating frequencies jammed. Al Jazeera Arabic news experienced this type of interference to their broadcasts in 2011.[27]

Even democratic countries have been tempted to try wholesale disconnection. In San Francisco, the Bay Area Rapid Transit system cut off cellphone coverage in four stations to prevent local residents from coordinating a protest.[28] In the UK, during the 2011 August riots, the government briefly considered turning off the BlackBerry network being used for communications, but eventually concluded that doing so would be inadvisable because the ability to use the Internet and social media to disseminate accurate information was too valuable to the police.[29]

All these efforts are possible because even in the many countries that do not operate a nationwide firewall, Internet access typically passes through a handful of chokepoints where government control can be exercised, including at the level of mobile network operators, Internet service providers, or large data centers. In January of 2011, US Senator Joseph Lieberman proposed that the president should have an Internet "kill switch" enabling him to shut down or seize parts of the US Internet in case of attack.[30]

These shutdowns are both a threat to legitimate protest and the realization of other human rights, which pose a specific and alarming problem for civil society organizations.

COMPROMISED USER ACCOUNTS

Two major types of problems arise when user accounts are compromised: first, that the attacker can access confidential information intended only for those users, and second, that the attacker can pose as one or more of those users, disrupting trust relationships, disseminating false information, even altering travel plans or cancelling the delivery of necessary supplies. We saw both of these problems in 2011.

User account compromises are often a result of one of the other attacks already described: man-in-the-middle attacks can harvest unencrypted user IDs and passwords and message contents; surveillance attacks that are assisted by technology companies

[17] http://topics.bloomberg.com/wired-for-repression/

[18] http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html

[19] http://www.bloomberg.com/news/2011-11-28/italian-firm-exits-syrian-monitoring-project-repubblica-says.html

[20] http://www.zdnet.co.uk/news/regulation/2011/12/08/eu-moves-to-stop-surveillance-tech-sales-to-despots-40094614/

[21] http://www.guardian.co.uk/technology/2011/nov/01/governments-hacking-techniques-surveillance

[22] http://www.npr.org/2011/12/14/143639670/the-technology-helping-repressive-regimes-spy

[23] http://www.bbc.co.uk/news/world-europe-12985082

[24] http://www.guardian.co.uk/world/2007/sep/27/burma.technology

[25] http://www.nytimes.com/2011/02/21/business/media/21link.html

[26] http://www.wired.co.uk/news/archive/2011-04/18/iran-halal-internet

[27] http://www.journalism.co.uk/news/al-jazeera-still-battling-interference-in-egypt-after-internet-blackout-lifted/s2/a542597/

[28] http://news.heartland.org/newspaper-article/2011/08/22/fcc-may-investigate-san-francisco-mobile-device-blackout

[29] http://www.telegraph.co.uk/technology/facebook/8765655/Facebook-and-Twitter-blackout-during-riots-would-threaten-public-safety.html

[30] http://www.cbsnews.com/8301-501465_162-20029302-501465.html

can harvest even the contents of some encrypted communications (for example, text messages sent by cell phone may be encrypted in transit but still readable by the network operator itself). In addition, accounts may be compromised when a user's machine is targeted by malware.

Finally, governments are in a position to compel service providers to disclose the real identities behind pseudonymous or apparently anonymous accounts; in the wake of Wikileaks' release of diplomatic cables, for example, the US State Department pressured Twitter and Google to turn over user account information under the Electronic Communications Privacy Act; Google responded by disclosing the private data of a Wikileaks volunteer without a search warrant.[31]

The types of accounts that are vulnerable to this type of attack are many and varied: email, social networks, website administration, internal networks, the passphrases protecting cryptographic software, and web transaction accounts in general (ecommerce, banking, or travel sites, for example). User account compromises are exacerbated (and the potential for identity fraud of all types greatly expanded) if the user, uses a single password across multiple accounts, which many do.

Once an account is compromised, the attacker can do anything from reading and copying email to mounting a more elaborate attack on an entire organization — and perhaps beyond — from just one, trusted but compromised node. An example of this type of escalating attack in the commercial world is the March 2011 breach of the security company RSA; a handful of low-level employees were targeted with malware and the resulting security hole compromised security systems in major organizations worldwide.[32, 33]

In the years leading up to the 2010 Tunisian revolution, protesters used Facebook as a resource, opening personal pages after many blogs had been shut down. On these pages they posted video clips and kept close track of developments. Previously, the site was simply blocked. In January 2011 a countrywide man-in-the-middle attack was revealed that harvested users' Facebook passwords. The attack worked by intercepting the Facebook login page (http rather than https), inserting a small piece of JavaScript that read off the user name and password and sent them to a bogus page on Facebook, then logging all requests for that page.[34] When after about five days, Facebook's engineers realized what was happening, the company took steps to shut it down.[35] Yahoo! and Gmail users were similarly targeted; in some cases the contents of email messages were replaced with threats or apparently random ads.[36]

A more direct and personal method of obtaining user credentials includes the use of torture, threats, and abuse. In May, organizers of the Syrian Revolution 2011 Facebook page reported that after a campaign of mass detentions, protesters who had been uploading video clips were tortured to force them to reveal their Facebook user names and passwords.[37]

WEBSITE DEFACEMENTS AND CYBER VANDALISM

The frequency of politically motivated attacks of this type is on the rise. After reporting on the anti-government protests in Egypt in February 2011, the Al Jazeera Arabic news website was defaced with the message 'Together for the collapse of Egypt' and a link to another website critical of Al Jazeera.[38] Another defacement occurring in the same month was carried out by the Iranian Cyber Army on the website of Voice of America (VOA). A message left on the site for Secretary of State Hillary Clinton read 'Hear the voice of oppressed nations' and called on the US to stop interfering in Islamic countries.[39] Yet another attack in February resulted in a Jordanian website being defaced after refusing to accede to the demands of security agents requesting the removal of a statement from 36 tribal chiefs calling for democratic and economic reforms.[40]

Throughout 2011 a group calling itself the Syrian Electronic Army carried out a number of defacements against the websites of organizations and individuals they perceived as supporting the revolution against the Syrian regime. Infowar Monitor detailed many of these attacks in a report published in June 2011. The report also details other forms of cyber vandalism carried out by the group including the repeated posting of pro-Assad messages on the Facebook pages of Nicolas Sarkozy, Barack Obama, ABC news, and others.[41, 42]

In December 2011, the website of the Indian National Congress was defaced. The attackers, possibly from Pakistan, replaced the image of the INC's leader, Sonia Gandhi, with a pornographic message.[43]

The methods used to perpetrate these defacement attacks include some of the other threats documented here, such as man-in-the-middle attacks and compromised user accounts. In other cases, the attacks build on known vulnerabilities in server software and/or insufficient attention to security on the part of the site

[31] http://www.readwriteweb.com/archives/google_hands_wikileaks_volunteers_gmail_data_to_us.php

[32] http://www.networkworld.com/news/2011/031811-rsa-warns-securid-customers-after.html

[33] http://www.networkworld.com/news/2011/080311-breach-securid-china.html

[34] http://www.thetechherald.com/articles/Tunisian-government-harvesting-usernames-and-passwords

[35] http://www.theregister.co.uk/2011/01/25/tunisia_facebook_password_slurping/

[36] http://www.techdirt.com/articles/20111213/11181117066/former-tunisian-regime-goes-beyond-spying-internet-traffic-to-rewriting-emails-more.shtml

[37] http://www.telegraph.co.uk/news/worldnews/middleeast/syria/8503797/Syria-tortures-activists-to-access-their-Facebook-pages.html

[38] http://www.journalism.co.uk/news/al-jazeera-site-hacked-by-opponents-of-pro-democracy-movement-in-egypt/s2/a542649/

[39] http://thehackernews.com/2011/02/voice-of-america-voa-website-hacked-by.html

[40] http://livenews.thestar.com/Event/Arab_World_Today/8907858

[41] http://www.infowar-monitor.net/2011/05/7349/

[42] http://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/

[43] http://www.france24.com/en/20111209-hackers-deface-profile-indias-sonia-gandhi

owner or host.

Some new forms of cyber vandalism appeared in 2011 posing a direct threat to civil society. The hack of HB Gary by 'Anonymous' revealed US federal government plans to weaponize social media by creating software to generate large numbers of fake user profiles, the so called 'sock-puppet army', to be operated to drown out conversations online with messages pushing a pro-government viewpoint.[44, 45] A congruent tactic of 'Hashtag junking' was used in December 2011 during the Russian elections. An automated system utilizing a large number of computers flooded Twitter with pro-government tweets using the hashtag '#triumphalnaya', effectively destroying the quality of the conversation on the topic previously associated with the hashtag.[46]

DATA LEAKAGE

In 2011, The Metropolitan police in Britain began using software that correlates large data sets from surveillance technology with data from social networking sites to predict public order disturbances.[47] The adoption of Social Network Analysis (SNA) practices and tools soared among law enforcement agencies worldwide during 2011. The rise of SNA means it no longer requires a lot of time-consuming physical work to study the relationships among a group of activists or political opponents. What would have previously required an organization to eavesdrop on phone calls, intercept postal mail, break into offices to read files, mount a surveillance operation, or capture and torture one or more identifiable members of their opponent organization, may be achieved today without leaving the office by simply studying the target's circles of Facebook friends and email contacts. The detectives in the 2010 documentary *Erasing David*, who were tasked with locating the David of the title, noted this. As part of their efforts, they sent friend requests to all of David's Facebook list; a few accepted, and they went to several of his friends' parties hoping he'd show up (he didn't).

For this reason, data leakage is a very serious threat to civil society, especially those at the front lines. If their identities are revealed it could mean incarceration, torture, or even death.

Data leakages in 2011 occurred in many ways, some of them already discussed here. One or more compromised user accounts or machines may enable attackers to gain further access to the information available to those users and forward it to any destination. Man-in-the-middle attacks harvest traffic data such as email contacts and web addresses as well as content such as messages and phone calls. Wireless access compromise networks by making it easier for an outsider to surreptitiously monitor the network. Small devices that attach to the network such as smart phones open up access for an attacker if the phone is lost or stolen. Finally, all devices that store data are vulnerable to theft or confiscation, followed by forensic examination to extract sensitive information. This information can then be used in may ways, from tracking down people to identity theft.

In the case of Public Space, a Caracas-based NGO campaigning for freedom of expression, two robberies saw the NGO's electronic devices taken, along with (in the second attack) surveillance videos and equipment from the first attack.[48] Similarly, in 2010 computers were stolen from the Kenya-based International Centre for Policy and Conflict, which was working with the International Criminal Court to examine violence after the 2007 Kenya election. In November 2011, the hacker group Team Poison attacked a server belonging to the United Nations Development Program and later published online a long list of the user IDs and passwords stored on it.[49]

Insiders also pose a threat in this type of attack, as an enormous amount of data can be copied covertly onto USB sticks, flash cards, or DVDs and removed from the premises almost undetectably. The 250,000 diplomatic cables published by Wikileaks, for example, leaked out after being copied onto a DVD by a single, low-level army private. If it poses a threat to the military of the most powerful country in the world, then likely it is a threat to every organization.

DENIAL OF FUNDING

The history of the Internet has been one of increasing consolidation so that in many categories one or two large players dominate the landscape. The result is to create an infrastructure with what engineers call "central points of failure." For civil society, one of those central points is funding: in any given country there are very few widely used and trusted channels by which individuals can transfer funds electronically to an organization they wish to support.

Accordingly, in the wake of the release of diplomatic cables, when the US and some EU governments were condemning Wikileaks, PayPal, Mastercard, and Visa opted to freeze Wikileaks' accounts and Amazon suspended its hosting ("cloud") services.[50] In other cases, Paypal's rules have seemed to outside observers to be arbitrary and unpredictable. In October 2011, PayPal froze the account of Diaspora (an effort to build an open-source alternative to Facebook) during a drive to raise funding to continue its work.[51] In March 2010, PayPal similarly froze the account of Cryptome,[52] a longstanding (founded 1996) repository of information on

[44] http://www.dailykos.com/story/2011/02/16/945768/-UPDATED:-The-HB-Gary-Email-That-Should-Concern-Us-All

[45] http://www.thetechherald.com/articles/Anonymous-Government-contractor-has-weaponized-social-media

[46] http://www.bbc.co.uk/news/technology-16108876

[47] http://www.guardian.co.uk/uk/2011/may/11/police-software-maps-digital-movements/print

[48] http://computersecurity.blogspot.com/2011/11/texas-computers-stolen-httpknightcenter.html

[49] http://ngosecurity.blogspot.com/2011/11/un-server-hacked.html

[50] http://www.bbc.co.uk/news/business-11945875

[51] http://www.techdirt.com/articles/20111213/11181117066/former-tunisian-regime-goes-beyond-spying-internet-traffic-to-rewriting-emails-more.shtml

[52] http://www.fastcompany.com/1575296/now-paypal-goes-for-cryptome-suspends-account

surveillance, cryptography, and free speech after a burst of publicity over a complaint from Microsoft that had briefly caused Cryptome's website to be taken down brought the site an unusual surge in donations. In the Cryptome case, PayPal backed down and apologized relatively quickly; as of December 2011 PayPal had rejected Diaspora's appeal and Diaspora was still waiting for the company to give a reason.

These cases are inspiring the development of alternatives such as Flattr[53,54] and Stripe[55], but cutting off the payment methods used by the mainstream can effectively and abruptly throttle an organization's funding. Given the right timing — during a well-publicized funding drive, or at a moment of particular need — such tactics pose a serious threat to a civil society organization's survival.

TAKEDOWN NOTICES

Takedown notices began as a compromise. Governments and other organizations such as the entertainment industry wanted to have some ability to control copyright and legal violations, while ISPs and hosting organizations argued that they could not possibly police their users' postings and uploads effectively. In the US, in any case, requiring them to do so would arguably violate the First Amendment prohibition on prior restraint for publication. Accordingly, a series of legal cases in the US and EU established a system of notice-and-takedown, under which ISPs and other types of hosts avoid liability for their users' activities provided that when they are notified that they are hosting material that violates the law, they take it down.

This system is imperfect because, as providers must make a determination over the legality of content whilst simultaneously having to consider their own liability (should they fail to take down infringing or otherwise illegal content expeditiously). Anxious to avoid legal liability, service providers typically take down material as soon as there is a complaint and only investigate afterwards if the customer protests, but even then, in most jurisdictions, the provider is immunized from a lawsuit from its customer. This mechanism can, therefore, be abused by closed and semi-closed governments to cloak censorship of opposition voices under the veil of legal necessity. Anything from seizing a domain to removing hosted content or an entire website may be explained away with an excuse such as copyright infringement or a violation of the service provider's Terms of Service.

The practice seems set to grow. In India in 2011, the Bangalore-based Centre for Internet and Society tested the new Information Technology (Intermediaries Guidelines) Rules by sending flawed takedown requests to seven major websites, reporting that six "over-complied".[56] The Chilling Effects website documents thousands of notices inappropriately issued under the US's Digital Millennium Copyright Act (1998).[57] In this area, Google has provided a considerable amount of transparency; early in 2011 it began sending the Chilling Effects Clearinghouse copies of the takedown notices it receives for the Android Marketplace, and it also publishes a biannual report on the government requests it receives to identify users and to remove material from view on all of its services. [58]

In March of this year, several Egyptian protesters broke into the Nasr City offices of the Egyptian State Security, a building housing one of Mubarak's most infamous torture facilities. Egyptian blogger Hossam Arabawy came into possession of a CD of photos of officers, which he then uploaded to the Yahoo! Service Flickr. Shortly afterwards, Flickr removed the photos, citing a guideline in its Community Guidelines (Terms of Service) which state that users may only upload their own content.[59] It's important to note that this content was taken down through a terms of service violation, not a notice of copyright infringement (although that could have potentially been alleged as well), which shows the power that these private contractual agreements (between providers and their users) have over the free flow of information.

[53] http://eu.techcrunch.com/2010/12/08/wikileaks-continues-to-fund-itself-via-tech-startup-flattr/

[54] http://flattr.com/

[55] https://stripe.com/

[56] http://cis-india.org/private-censorship-making-online-content-disappear-quietly

[57] http://www.chillingeffects.org/

[58] http://www.google.com/transparencyreport/

[59] http://techcrunch.com/2011/03/11/flickr/

//

ACCESS TECH'S APPROACH TO THREAT MITIGATION

Access Tech works to develop and promote technology to improve open access and free, full, and safe participation in society. We endeavor to build the technical capacity of all individuals, particularly members of civil society living behind the firewall. This includes direct action to affect immediate relief where needed, and comprehensive long term undertakings to affect robust change into the future. We assist civil society to protect themselves, secure their communications, and improve the capability of activists on the ground in communications blackout scenarios. Access Tech authors educational documents to assist civil society to become more aware of the threats they face and provide instruction on how to mitigate those threats. Listed below are a few samples of material Access Tech has produced. These materials are available online at: https://www.accessnow.org/docs.

DEFENDING AGAINST DENIAL OF SERVICE ATTACKS

Civil society websites are under attack. This step-by-step guide is designed to assist technical staff in defending websites against these attacks.

DoS INSURANCE SCHEME

While civil society often bears the brunt of DoS attacks they rarely can afford effective Denial of Service Protection (DoSP) services. This proposal is aimed at solving that quandary.

MAN IN THE MIDDLE ATTACKS ALERT

Widespread compromises of civil society members from MitM attacks have started to come to light. This alert gives clear instructions to navigate this complex issue safely.

PROTECTING YOUR SECURITY ONLINE

Individuals and organizations use the internet to further civil rights. This guide gives pointers to many aspects of cyber security to keep everyone safe online.

HOW TO TRAVEL SAFELY

Human rights advocates travel frequently. This guide outlines steps that can be taken to travel safely with digital information.

PGP/GPG GUIDE

Activists and NGO staff are talking and emailing online, but often over insecure channels. This comprehensive guide illuminates how to communicate via email securely.

DIGINOTAR RESPONSE

One of the most fundamental online security mechanisms is under threat. This mechanism is relied on heavily by civil society to secure communications. This paper outlines possible avenues to add robustness to the overall SSL system.

//

For more information, please visit **https://www.accessnow.org**
or email **soc@accessnow.org (PGP Key ID: 0xF08D380A)**