How To Communicate Securely in Repressive Environments

Important: Please check the excellent comments provided by *iRevolution* readers below for additional tactics/technologies and corrections. The purpose of this blog post was to inform and elicit feedback so thank you very much for improving on what

INTRODUCTION

Core to effective strategic nonviolent action is the need to remain proactive and on the offensive; the rationale being that both the resistance movement and repressive regime have an **equal amount of time** allocated when the show-down begins. If the movement becomes idle at any point, this may give the regime the opportunity to regain the upper hand, or vice versa. The same principle is found in Clausewitz's writings on war.

Nonviolent resistance movements are typically driven by students, i.e., young people, who are increasingly born digital natives. With expanding access to mobile phones, social networking software and online platforms for user-generated content such as blogs, the immediate **financial cost** of speaking out against repressive regimes is virtually nil. So resistance movements are likely to make even more use of new communication technology and digital media in the future. In fact, they already are.

At the same time, however, the likelihood and consequences of getting caught are high, especially for those political activists without any background or training in digital security. Indeed, recent research by Digital Democracy research suggests that **organizational hierarchies** are being broken down as youth adopt new technologies. While this empowers them they are also put at risk since they don't tend to be as consequence-conscious as their adult counterparts.

EMPIRE STRIKES BACK

It is no myth that repressive regimes are becoming increasingly more savvy in their ability to effectively employ sophisticated filtering, censoring, monitoring technologies (often courtesy of American companies like Cisco) to crack down on resistance movements. In other words, political activists need to realize that their **regimes are becoming smarter** and more effective, not dumber and hardly clueless.

That said, there are notable—at times surprising—loopholes. During the recent election violence in Iran, for example, facebook.com was blocked but not facebook.com/home.php. In any case, repressive regimes will continue to block more sites impose information blockades because they tend to view new media and digital technologies as a threat.

Perhaps technologies of liberation are a force more powerful?

In order to remain on the offensive against repressive regimes, nonviolent civil resistance movements need to ensure they are **up to speed** on digital security, if only for defense purposes. Indeed, I am particularly struck by the number of political activists in repressive regimes who aren't

aware of the serious risks they take when they use their mobile phones or the Internet to communicate with other activists.

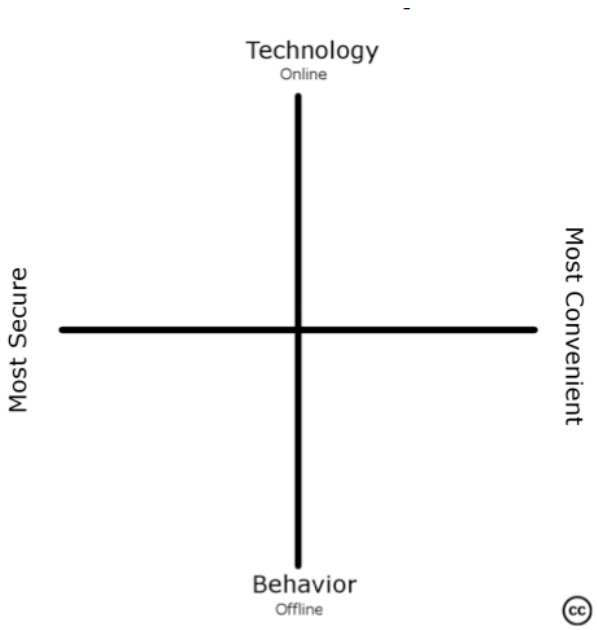
ADAPTIVE LEARNING

One way to stay ahead is to make the learning curve less steep for political activists and to continually update them with the latest tested tactics and technologies. To be sure, one way to keep the upper hand in this cyber game of cat-and-mouse is to continue adapting and learning as quickly as possible. We need to ensure that **feedback mechanisms** are in place.

There are clearly trade-offs between security and convenience or usability, particularly in the context of technologies. As DigiActive notes in the graphic below, the most secure tactics and technologies may not be the most convenient or easy to deploy. **Most political activists are not tech-savvy**.

This means that digital activists need to design tactics and technologies that are easy to learn and deploy.

The tactics and technologies listed in the next sections fall into all four different quadrants to one extent or another. It is important that political activists *at minimum* master the easy and convenient digital security tactics and technologies identified in this blog post.



Recall that both sides are allocated an equal amount of time to plan and execute their operations. **Accelerating the learning process** is one way for activist networks to remain pro-active and stay ahead of the curve. This is in part is the role that DigiActive seeks to play. Unlike the hierarchical, centralized structures of repressive regimes, networks have more flexibility and feedback loops, which make them more adaptable.

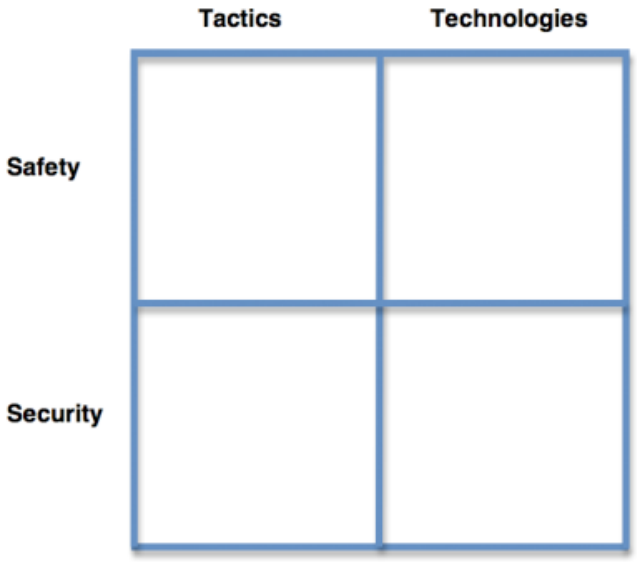
The normative motivation behind my research on digital resistance is based on the recognition by "many scholars and practitioners [...] that the techniques associated with strategic nonviolent social movements are greatly **enhanced by access** to modern information communication technologies, such as mobile telephony, short message service (SMS), email and the World Wide Web, among others" (Walker 2007).

The potential to leverage those techniques is what makes Digital Security so important to integrate in the **strategic and tactical repertoire** of civil resistance movements.

DIGITAL SECURITY

I define digital security (DS) in the context of digital resistance as the art and science of staying safe when communicating in non-permissive environments. The reason I call it **both an art and a science** is to emphasize that *both* tactics and technology play an important role in staying safe when facing repression.

So the DS framework I want to propose is **two-pronged**: tactics vs. technology, and safety vs. security. I call it the 4-square approach for obvious reasons:



- **DS tactics:** these can be "technology free" tactics as well as tactics that apply communication technology.
- **DS technologies:** these include both high-tech and low-tech technologies that are designed to improve safe and secure communication in repressive environments.
- **Personal safety:** in this context refers to physical, personal safety when communicating in non-permissive environments.

- **Data Security:** refers to the security of the data when communicated from one devise to another.

As the graphic above suggests, personal safety and data security are a function of both tactics and technologies. For example, data security is best ensured when combining tactics and technologies.

What follows is a **list of tactics and technologies** for communicating safely and securely in repressive environments. The list is divided into technology categories and the bullet points are listed in order of relative convenience and easy to more complicated but more secure.

Note that the information below is in no way meant to be exhaustive, so please do **send suggestions!** (See also the conclusion for a list of reference and suggestions on further reading).

DIGITAL SECURITY TACTICS

As mentioned above, DS tactics come as both **technology-free tactics** and tactics that relate to communication technology. For example, making sure to pay for a sim card in cash and out of sight of security cameras is a technology-free tactic that increases the chances of staying safe. Removing the batteries from your mobile phone to prevent it from being geo-located is a tactic that relates to the technology and also increases your safety.

DS tactics can also improve data security when communicating information. "Sneakernet" is a technology-free tactic to share information. The term is used to describe tactics whereby the transfer of electronic information such computer files is done by physically carrying removable media such as hard drives and disk drives. In contrast, using encryption software for mobile phones is a tactic that **uses technology**. The communication may be intercepted by eavesdroppers but they may be unable to decipher the message itself.

These tactics are listed below along with a number of other important ones. Please keep in mind that tactics are case- and **context-specific**. They need to be adapted to the local situation.

- **Mobile Phones**
  - Purchase your mobile phone far from where you live. Buy lower-end, simple phones that do not allow third-party applications to be installed. Higher-end ones with more functionalities carry more risk. Use cash to purchase your phone and SIM card. Avoid town centers and find small or second-hand shops as these are unlikely to have security cameras. Do not give your real details if asked; many shops do not ask for proof of ID.
  - Use multiple SIM cards and multiple phones and only use pay-as-you go options; they are more expensive but required for anonymity.
  - Remove the batteries from your phone if you do not want to be geo-located and keep the SIM card out of the phone when not in use and store in separate places.Use your phone while in a moving vehicle to reduces probability of geo-location.
  - Never say anything that may incriminate you in any way.
  - Use code.
  - Use Beeping instead of SMS whenever possible. Standard text messages are visible to the network operator, including location, phone and SIM card identifiers. According to this recent paper, the Chinese government has established 2,800 SMS surveillance centers around the country to monitor and censor text messages. The Chinese firm Venus Info Tech Ltd sells real-time content monitoring and filtering for SMS.

- Use fake names for your address book and memorize the more important numbers. Frequently delete your text messages and call history and replace them with random text messages and calls. The data on your phone is only deleted if it is written over with new data. This means that deleted SMS and contact numbers can sometimes be retrieved (with a free tool like unDeleteSMS. Check your phone's settings to see whether it can be set to not store sent texts messages and calls.
- Eavesdropping in mobile phone conversations is technically complicated although entirely possible using commercially available technology. Do not take mobile phones with you to meetings as they can be turned into potential listening/tracking devices. Network operators can remotely activate a phone as a recording device regardless of whether someone is using the phone or whether the phen is even switched on. This functionality is available on US networks.
- Network operators can also access messages or contact information stored on the SIM card. If surveillance takes place with the co-operation of the operator, little can be done to prevent the spying.
- Mobile viruses tend to spread easily via Bluetooth so the latter should be turned off when not in use.
- Using open Bluetooth on phones in group situations, e.g., to share pictures, etc., can be dangerous. At the same time, it is difficult to incriminate any one person and a good way to share information when the cell phone network and Internet are down.
- Discard phones that have been tracked and burn them; it is not sufficient to simply destroy the SIM card and re-use the phone.

- **Digital Cameras**
  - Keep the number of sensitive pictures on your camera to a minimum.
  - Add plenty of random non-threatening pictures (not of individuals) and have these safe pictures locked so when you do a "delete all" these pictures stay on the card.
  - Keep the battery out of the camera when not in use so it can't be turned on by others.
  - Practice taking pictures without having to look at the view screen.

- **Computers/Laptops**
  - Use pass*phrases* for all your sensitive data.
  - Keep your most sensitive files on flash disks and find safe places to hide them.
  - Have a contingency plan to physically destroy or get rid of your computer at short notice.

- **Flash disks**
  - Purchase flash disks that don't look like flash disks.
  - Keep flash disks hidden.

- **Email communication**
  - Use code.
  - Use pass*phrases* instead of passwords and change them regularly. Use letters, numbers and other characters to make them "cOmpLeX!". Do not use personal information and changer your passphrases each month. Do not use the same password for multiple sites.
  - Never use real names for email addresses and use multiple addresses.
  - Discard older email accounts on a regular basis and create new ones.
  - Know the security, safety and privacy policies of providers and monitor any chances (see terms of service tracker).

- **Browsers and websites**
  - Turn off java and other potentially malicious add-ons.

- Learn IP addresses of visited websites so that history shows only numbers and not names.
- When browsing on a public computer, delete your private data (search history, passwords, etc.) before you leave.
- When signing up for an account where you will be publishing sensitive media, do not use your personal email address and don't give personal information.
- Don't download any software from pop-ups, they may be malicious and attack your computer or record your actions online.
- Do not be logged in to any sensitive site while having another site open.

- **VoIP**
  - Just because your talking online doesn't mean you are not under surveillance.
  - As with a cell or landline, use code do not give salient details about your activities, and do not make incriminating statements.
  - Remember that your online activities can be surveilled using offline techniques. It doesn't matter if you are using encrypted VOIP at a cyber cafe if the person next to you is an under-cover police officer.
  - When possible, do not make sensitive VOIP calls in a cyber cafe. It is simply too easy for someone to overhear you. If you must, use code that doesn't stand out.

- **Blogs and social networking sites**

  - Know the laws in your country pertaining to liability, libel, etc.
  - When signing up for a blog account where you will be publishing sensitive content, do not use you personal email address or information.
  - In your blog posts and profile page, do not post pictures of yourself or your friends, do not use your real name, and do not give personal details that could help identify you (town, school, employer, etc.).
  - Blog platforms like wordpress allow uses to automatically publish a post on a designated date and time. Use this functionality to auto-publish on a different day when you are away from the computer.
  - On social networks, create one account for activism under a false but real-sounding name (so your account won't be deleted) but don't tell your friends about it. The last thing you want is a friend writing on your wall or tagging you in a photo and giving away your identity.
  - Even if you delete your account on a social networking site, your data will remain, so be very careful about taking part in political actions (i.e., joining sensitive groups) online.
  - Never join a sensitive group with your real account. Use your fake account to join activism groups. (The fake account should not be linked to your fake email).
  - Don't use paid services. Your credit card can be linked back to you.

- **File sharing**
  - Use a shared Gmail account with a common pass*phrase* and simply save emails instead of sending. Change passphrase monthly.
  - For sharing offline, do not label storage devices (CDs, flash drives) with the true content. If you burn a CD with an illegal video or piece of software on it, write an album label on it.
  - Don't leave storage devices in places where they would be easily found if your office or home were searched (i.e., on a table, in a desk drawer).

- Keep copies of your data on two flash drives and keep them hidden in separate locations.
- When thinking of safe locations, consider who else has access. Heavily-traveled locations are less safe.
- Don't travel with sensitive data on you unless absolutely necessary. If you need to, make sure to hide it on your person or "camouflage" it (label a data CD as a pop music CD). See Sneakernet.

- **Internet Cafes**
  - Assume you are being watched.
  - Assume computers at cyber cafes are tracking key strokes and capturing screenshots.
  - Avoid cyber cafes without an easy exit and have a contingency plan if you need to leave rapidly.

DIGITAL SECURITY TECHNOLOGIES

When combine with the tactics described above, the following technologies can help you stay safe and keep your data relatively more secure.

- **Mobile phones**
  - Use CryptoSMS, SMS 007 or Kryptext to text securely (this requires java-based phones).
  - Use Android Guardian as soon as it becomes available.
  - Access mobile versions of websites as they are usually not blocked. In addition, connecting to mobile websites provides for faster connections.

- **Digital cameras**
  - Use scrubbing software such as: JPEG stripper to remove the metadata (Exif data) from your pictures before you upload/email.
  - Have a safe Secure Digital Card (SD) that you can swap in. Preferably, use a mini SD card with a mini SD-SD converter. Then place the mini SD into a compatible phone for safekeeping.

- **Computers/Laptops**
  - Use an effective anti-virus program and ensure it updates itself online at least once a day: TMIS, McAfee, Symantec/Norton, AVG, Avira, NOD32, Kaspersky.
  - Do not use illegal, cracked, hacked, pwned, warez software.
  - Keep your software programs (operating systems, productivity suites, browsers) up-to-date with the latest software updates.
  - Use software to encrypt your hard drive: Bitlocker, TrueCrypt, PGP Whole Disk Encryption, Check Point, Dekart Private Disk.
  - Use a different file type to hide your sensitive files. For example, the *.mov* file extension will make a large file look like a movie.
  - Mac users can use Little Snitch to track all the data that goes into and out of your computer.
  - From a technical perspective, there's no such thing as the delete function. Your deleted data is eventually written over with new data. There are two common ways to wipe sensitive data from your hard drive or storage device. You can wipe a single file or you can wipe all of the 'unallocated' space on the drive. Eraser is a free and open-source secure deletion tool that is extremely easy to use.

- **Flash disks**

- StealthySurfer USB Flash Drive
- The secure browsing Tor software can be installed on flash disk.
- Using a USB watch calls less attention as do the USB ear rings and this credit card USB flash disk.

- **Email communication**
  - Use *https* when using Gmail.
  - Use encrypted email platforms such as Hushmail and RiseUp.

- **Browsers and websites**
  - Use Firefox and get certain plugins to follow website tracking such as ghostery and adblock, adart to remove ads/trackers.
  - User Tor software or Psiphon to browse privately and securely.
  - I shan't list access points for secure browsers, Proxy servers and VPNs here. Please email me for a list.
  - Always use *https* in "Settings/General/Browser Connection."

- **VoIP**
  - Use Skype but not TOM Skype (Chinese version). Note that Skype is not necessarily 100% secure since no one has access to the source code to verify.
  - Off The Record (OTR) is a good encryption plugin. For example, use Pidgin with OTR (you need to add the plug-in yourself).
  - Gizmo offer encryption for voice conversations, and then only if you are calling another VoIP user, as opposed to a mobile or landline telephone. However, because neither application is open-source, independent experts have been unable to test them fully and ensure that they are secure.
  - Adium is a free IM application for Macs with built-in OTR encryption that integrates most other IM applications.

- **Blogs and social networking platforms**
  - There are no safe social networks. The best way to be safe on a social network is fake account and a proxy server.
  - The anonymous blogging platform Invisiblog no longer exists, so the best bet now is WordPress + Proxy (preferably Tor) + anonymity of content.
  - Log out of facebook.com when not using the site.

- **File sharing**
  - Use Drop.io to create a private, secure media sharing site.
  - Use BasecampHQ with secure/SSL option to create more specific usernames and passwords for each user or remote site.

- **Internet Cafe**
  - Tor can be installed on flash disk and used at Internet cafe and also used from LiveCDs if flash drives are not allowed.

- **Other potential tech**
  - LiveScribe (see explanation here).
  - FreedomFone

CONCLUSION

The above material was collected in part from these sources:

- Tactical Tech's Mobiles-in-a-Box and Security-in-a-Box;
- MobileActive's Mobile Security
- FreeBeagles;
- FLOSS Manuals;
- Feedback from DigiActive and Digital Democracy;
- Personal experience and that of other colleagues in the field.

As mentioned above, please send suggestions and/or corrections as well as updates. And again, please do check the comments below. Thanks!

Patrick Philippe Meier

109 RESPONSES TO HOW TO COMMUNICATE SECURELY IN REPRESSIVE ENVIRONMENTS

This is a great explanation of the need for more awareness of security risks when using digital tools for activism – as well as a great compilation of resources and tools. It is always important to consider safety and security risks when assessing any tactic – including tech tactics!

Here's some very valuable feedback I received from a knowledgeable colleague:

* Many countries now require providing positive ID when buying a GSM SIM card (even a prepaid one). Possible solution: have a visiting tourist show their passport for you? (I've done this for folks in repressive countries.)

* If someone has physical access to your phone, they can install a "remote microphone activation" program onto it, but unless this has been done, as far as I know it's not possible to "turn a mobile phone into a listening device."

* I don't agree with your proposition to keep sensitive files on USB thumbdrives. Too many people who do that lose them. The important thing is to encrypt sensitive data, and invisibly encrypt super-sensitive data, and if you're really paranoid, make sure you have some only-slightly-sensitive encrypted data you can "be forced to give up" in order to be believable when you deny the existence of your highly-sensitive invisible data.

* I also don't agree much with the idea of using code in e-mails, not because I think it's wrong, but because it over-complicates something that can be kept simple (encrypt). Yes, I can see the justification: what if they get your e-mail from the person you're communicating with?—but if that's happened, you're probably already sunk. It's about balancing complication with usability.

* I don't agree with turning off JavaScript. Again, this is a tradeoff, but if you turn off Java, you can't use YouTube, etc. etc. etc. Similarly, I don't think it's reasonably to recommend memorizing IP addresses (aside from being impractical, because IP addresses change all the time).

* I don't agree with "don't talk openly about secret things via VoIP." Again, tradeoff. I think the important thing to understand about VoIP is simply that it's far more secure than using a "normal" phone.

* I've never seen anyone successfully encrypting SMSs. I'm not saying don't do it, nor that it's impossible.

* I've never heard of Skype being cracked. Arguably, that's the same situation as with e.g. Pidgin. I think the whole "it's open source, therefore it's safe" is a little exaggerated. But I know there are lots of people who disagree strongly!

Great work – though I would move TOR out of just the Internet Cafe area and as a general tool to be used whenever accessing the Internet.

I would also be worried about any use of a cell phone – at the end of they day, it is trackable by both financial records and location information based on the cell network; I've discussed some of the downfalls of mobiles here:

http://joncamfield.com/blog/2009/05/after_the_sms_honeymoon_update.html

A thorough and commendable survey of techniques and technologies, Patrick. Truly eye-opening. It points out the need, sad to say, to remain proficient in pre-digital forms of information sharing. As law enforcement imposes greater penalties on the use of digital technology for anything even just appearing to be subversive, revolutionary, or simply unsanctioned, the burden approaches a tipping point where the inclination will be to not use the technology.

When I was in Sweden during the later George W. years, I was reluctant to involve anyone at home (in the USA) in my online communications in the sure knowledge that we would be spied upon.

Now that I know everyone is spied upon in the US, at home and abroad, I don't have that worry. Now I can act courageously knowing there's no easy way out.

In a truly repressive regime, one has to be especially careful — and then the storm troopers have won. It's really a dilemma.

Patrick, I have a few observations for you. First, you advise "learn IP addresses of visited websites so that history shows only numbers and not names" however you should be aware that it is a relatively trivial matter to covert an IP address back to an DNS name and thereby identify the website visited. Using an IP address will only deter the least sophisticated snoop and may give a false sense of security.

Using a shared "save, don't send" gmail account does not/not provide any security. The information in the message is still sent from your computer to the gmail server and from the server to the computer of anyone else who reads messages on that account.

Using "code" during phone conversations can lead to a false sense of security. Every security service in the world knows this trick. It won't take them long to figure out what you really mean by 'friends', 'party', and 'bulldogs'.

Encrypting a hard drive only provides protection if the owner has been separated from his/her computer and is in a safe location. Security services rarely find it necessary to resort to elaborate computer forensics to gain access to the information if they also have the computer's owner. Most people 'voluntarily' give up their passwords in relatively short order.

One final note of caution, if the authorities catch you using several of the more sophisticated methods you've mentioned you will be marked as a serious player and will garner "serious" attention in return.

> Many thanks for taking the time to share your feedback and insights. On general false sense of security, anyone could argue that for any of the tactics and technologies collected from the different references I site.
>
> *IP addresses – yes, of course it's easy to convert them back to a DNS name. As you may have read in my introduction to the tactics/technologies, they vary from convenience to security, so there's a wide range of options provided, each with trade-off's. I hope I had made that point clear enough but I should perhaps go back and put in bold.
>
> *Gmail/Send – thanks for the correction.
>
> *Code – again, convenience vs security, using code does not mean every word you exchange is code. Only a handful of words can be code. And the point is to regularly change that code anyway, and not to have extensive conversations using said code. My thought is 2-3 minutes at most.
>
> *Encryption – very good point.
>
> *Sophisticated methods – another very good point.
>
> Thanks again, Kevin.
>
> It is very simple to block access to any specific http URL, while leaving access to to other URLs on the same host or in the same domain. simple firewall technology provides this, and it would be trivial for a telecom company to provide this on a large scale.
>
> so yes, they could block specific searches at search.twitter.com while leaving the rest open.
>
> what is difficult is for security forces to identify and block all services as quickly as they can be made available. proxies and tunnels can be used to obfuscate the actual addresses that are being accessed.

Really wonderful list of creative tactics. I especially like the approaches that are less technical and more behavioral. The models are great too; very understandable.

Some friendly suggestions:

- I would really like to see some of the technologies/behaviors plotted on the 4 square (though it makes plenty of sense as an evaluative model on its own; perhaps placing some logos would help spice it up).

- Can you cite the anecdote about facebook.com vs facebook.com/home? I'm interested in knowing if it is possible to block specific pages instead of domains. This is very relevant today because of a major rumor about the Iranian government blocking search.twitter.com/iranelections but no other results. I was quick to dismiss this as technically unfeasible (Im sure it's *possible* though, if you have total control over the data — just seems highly unlikely to me based on my understanding of DNS and censorship patterns).

- careful not to confuse java and javascript (your first comment); I disable java all the time, but javascript is increasingly a dependency for using the web (unfortunately).

- I would love to see a summary of the "most risky" behaviors or technologies. Given Kevin's excellent point about sophisticated behaviors attracting suspicion, it seems that the best approach for many activists would be to avoid some approaches altogether, unless you *really* need to use one approach.

> * Agreed on plotting the tactics/technologies on 4Square; hesitated because to some extent it depends who the user/reader is, folks come with different tech background and may find one tactic/tech easier than the other.
>
> * Following up with my contact to get citation for the facebook reference.
>
> * Thanks on the java vs javascript correction.
>
> * Good point about summarizing "most risky" tactics/technologies

Great post, Patrick — this is something I've been thinking about quite a bit and it is excellent to see such an extensive list of technology/tactics.

Thank you also to all for the comments, particularly Kevin T.

In addition to the technology/tactics, I think it is important to consider the end user. As you note, "most political activists are not tech-savvy". These individuals need to fully understand the risk they take by engaging in dissent (obviously) and also the additional risk they may take on by using these tactics to obscure their actions. If they are found out — and none of these are so technologically-advanced that they couldn't be detected by a sophisticated regime or determined agent — having used *some* of these techniques may be enough to implicate. Question is, how high are the stakes? Is anyone actually listening in? These contextual questions will inform any approach. Minimizing the trail of activists' communications seems to be the chief concern.

In any case, this is important information that people need to have.

An interesting note: many of the technologies built to make Western consumers' lives easier and more networked (GPS in cell phones and cameras) can also make activists' jobs harder.

Quick question — have you heard of a standalone camera (i.e. not a cameraphone) being remotely operated? The majority of point and shoot cameras do not have any networking capability (a very small minority have WiFi built in).

Excellent blog post on how to blog anonymously:

http://onlinejournalismblog.com/2009/06/16/7-ways-to-blog-anonymously/

http://www.frontlinedefenders.org/manual/en/esecman/intro.html

Some more excellent feedback from a colleague:

o Set a phone lock code to prevent others from quickly or easily accessing your phone.

o Remove phone serial numbers, such as the IMEI number, often located under the battery or phone casing to prevent immediate physical positive identification. Obvious obstruction in this way would suggest suspicious activity.

o Remember that flash disks can easily fail or break; know what is contained on the flash disk and what to do if data is lost.

o Use Firefox but not Internet Explorer whenever possible.

o Use XeroBank browser, an anonymous browser designed to run on both Tor and XeroBank anonymity networks.

> "Remove phone serial numbers, such as the IMEI number, often located under the battery or phone casing to prevent immediate physical positive identification. Obvious obstruction in this way would suggest suspicious activity."
>
> Is there any point in doing this ?
>
> Almost all mobile phones display the IMEI when given the international standard command sequence:
>
> *#06# [enter]
>
> Removing the battery, SIM card and then the sticky IMEI label is almost certain to leave DNA, fingerprint, chemical, dust or fibre forensic evidence, linking you to that particular handset.

> Every voice call, SMS text message or data call, is logged with the handset IMEI along with the IMSI phone number on the SIM card.
>
> It is possible to re-programme many model of mobile phone handset, ideally using standard “black market” mobile phone “unblocking” hardware or software, which tends to set each phone to the same IMEI.
>
> This is of course, illegal in many countries (up to 5 years in prison in the UK).
>
> “Remember that flash disks can easily fail or break; know what is contained on the flash disk and what to do if data is lost.”
>
> Physically losing small flash memory devices is a bigger problem.
>
> It is usually the connectors and circuit board tracks which fail, not the flash memory chip itself.
>
> Erasing flash memory securely is almost impossible – it is not affected by magnetism which would wipe out a floppy or hard disk. (N.B. some modern hard disks for portable computers now have a flash memory buffer, so even if you magnetically wipe them , your most recent, and probably most sensitive data may not have been wiped)
>
> Flash memory also tends to use algorithms to spread the read/write usage evenly across the memory cells, since when they hit the maximum limit, the data is permanently burned into them.
>
> Windows and Mac operating systems tend to create a local Wastebasket directory or folder on the flash memory device, from which it is trivial to recover “deleted” files from, and which many people are not aware of.
>
> This could be disastrous for deleted or amended versions of , say, your PGP Private Keyring, but otherwise encrypted container files (e.g. TrueCrypt volumes which do not have a separate unencrypted passphrase) or encrypted file systems should be ok.
>
> Thanks for the note, am not doing a PhD at Harvard but rather at Tufts.

Another good point from conversations with colleagues:

* You can use a regime’s ability to carry out monitoring/surveillance by deliberately producing disinformation and providing wrong information about meetings, protests, etc.

For fast and secure wipe of the entire hard drive in case of an emergency try Darik’s “Boot And Nuke”:

http://www.dban.org

A few extra hints as well, in particular in regards to cybercafes and meetings.

Personal safety:
1. Never carry anything that can be seen to be a weapon
2. Carry as little as possible
3. Avoid travelling alone, but travel with people who are unaware of your actual purpose.

Clothing:
There are two approaches you can take to make it difficult for people to recognize you. First is to be spotted, the second is to blend. If you are going for the spotting option, you must enhance the likelihood that what people will remember won't be you, but what you are wearing and what you are doing. If you are going for blending, then you are keeping as low a profile as possible.

Be Spotted:
1. Wear eye-catching accessories (thick rimmed glasses, knee-high rubber boots)
2. Apply dirt (never make-up) to your skin.
3. Practice a distinct body characteristic (running your hand through your hair, walking stooped)
4. Wear a double-sided jacket, a short t-shirt underneath a long shirt, or similar easy to carry replacements.
5. Carry a backpack full of random items (they should be worthless)

Usage:
Remember to act slightly differently than you normally would (cough loudly, etc.). Should people take an interest in you, find toilets or a similar public high-occupancy facility, taking care to leave your backpack outside of the facility and in plain sight. Quickly change inside, wash your skin, drop all eye-catching accessories, then walk back outside. Ignore the backpack and any attention it might have gathered. Remember, you're a different person now.

Blending:
1. Wear clothes in earthly tones (green, brown, sandy, etc.)
2. If you have a distinguishing characteristic – practice and get rid of it.
3. Act normally, but speak as little as possible.
4. Seek crowds, but stay near their edges.

Usage:
You're trying to be just another innocent bystander. It's not a bad idea to first study in detail the behaviour of everyday people in your particular country in order to get an idea of what the average person does in a particular situation. Learn this because it might be the difference between jail and freedom.

Excellent post as usual. Wish I could attend your presentation.

A couple of tools that I believe haven't been mentioned yet, but that are extremely useful for security:

- Martus – http://www.martus.org/: This encrypted database software designed by Benetech is an amazing tool for keeping sensitive data secure. For journalists, human rights documentation workers and others, I know of no better program for encrypting and databasing information.

- Crabgrass – https://we.riseup.net/crabgrass/about: Designed by the Rise-Up Collective, the idea behind Crabgrass is more secure social networking and collaboration. Although there are pros and cons to using it, activists working in repressive environments should know of it in case it is the right tool for their needs.

That's all for now. Again, very impressed by your post, Patrick, and the contributions in all of the comments.

regarding the storage media, Mini SD is obsolete. Micro SD (http://en.wikipedia.org/wiki/MicroSD) is much more suitable for "concealed carry". It's smaller (approximately 1/4 of a postcard, about 1mm thick), it's practically waterproof and currently comes in capacities of up to 32GB. Micro SD card readers are not much bigger than the card itself and can be practically hidden in plain sight. Here are a few examples:

htttp://www.dealextreme.com/details.dx/sku.21818

http://www.dealextreme.com/details.dx/sku.7106

http://www.dealextreme.com/details.dx/sku.25558

From http://bit.ly/dyugy:

How to post to Google Groups (old USENET) and send email anonymously using GPG encryption and anonymous remailer chains (see also http://email.about.com/cs/anonemailtips/qt/et041304.htm). If done thoughtfully and carefully, this provides a Twitter-like communications capability but with a secure (encrypted), anonymous email channel and no character limit. You can even attach photographs. Use the Twitter hashtag convention (#iranelection #neda) for easy searchability at Google Groups (http://groups.google.com/). Depending upon the remailer chain used, there will be a time lag of one or more hours before your message appears. This channel is not secure if your computer is susceptible to keystroke logging.

(rest at http://bit.ly/dyugy)

Making Gmail safe in Burma … http://him.civiblog.org/blog/_archives/2008/12/2/4003413.html

MAKE magazine ran a nice article on "how to acquire a bulletproof, anonymous online identity"

http://blog.makezine.com/archive/2009/06/flashback_make_yourself_invisible_0.html?CMP=OTC-0D6B48984890

There's a critical flaw in most of this. Regimes with enough power and legitimacy to criminalize free expression of speech have the authority to make the speakers disappear without a reason.

It's even worse in areas where encryption and data protection can easily be labeled, by the people attacking free speech, as traits of a child pornographer or the like.

My suggestion? Don't let secrets leave your head. If you're planning something with someone else that can be thwarted, organize it in person and act quickly.

> Hi Kevin, thanks for your comments. And yes, of course, I don't think anyone is suggesting that technology is the answer, hence my advocating for integrating civil resistance tactics/strategies with digital activism, i.e., repressive regimes have recourse to both forceful tactics and technologies. But resistance movements have recourse to nonviolent tactics (aka a force more powerful) and technologies as well. It's really important that digital activists become more familiar with tactics and strategies from civil resistance. Two follow up posts on this issue that may be of interest to you:
>
> http://irevolution.wordpress.com/2008/12/25/digital-resistance-between-digital-activism-and-civil-resistance
> http://irevolution.wordpress.com/2009/07/06/content-for-digital-activism-and-civil-resistance

Excellent article. As you suggested, I'll also post the feedback I sent you in person here.

- Tactics regarding mobile phones: The problem with pre-paid SIM cards is that after a little while, the identity of the owner can be established pretty easily based on their communication pattern. I don't have a smart suggestion how to get around this, but I thought you might want to mention it.

- TrueCrypt. You already mention this, however you do not explicitly point out the single best feature of TrueCrypt compared to the many other disk encryption programs out there: plausible deniability. This feature allows you to have a hidden encrypted partition wihtin the encrypted partition. And there is no way an attacker can tell whether the second encrypted partition exists or not.

http://www.truecrypt.org/docs/?s=plausible-deniability

- You suggest to "Learn IP addresses of key visited websites so that history shows only numbers and not names."
– Hostname:IP correspondences are not necessarily 1:1, a common case where this approach doesn't work is "virtual hosting", which simply means having several domains on one server. Many websites do not have their own IP but are implemented using VirtualHost on Apache http://httpd.apache.org/docs/1.3/vhosts/
If you type the IP instead of the domain name, you will not get to the domain you want to get to, but to some "root page" (typically the ISP)

- About posting to blogs, you might want to point out more explicitly that this is a specific case where anonymous access (such as using Tor) should be used.

- Hiding data CDs: you talk about writing album labels on the CDs, an even better thing to do is to burn a CD with several sections, the first is the audio section (so you can even just insert it into a CD player and play the "music CD") and then have a small data section after the music section. Even better, make the data section encrypted – then you can always pretend you didn't know it's there... after all you just bought a music CD at some street shop. (This might get you busted for copyright infringement but I guess in the kind of situation we're looking at that's the least of your worries.) This is a technique I'm personally using a lot and it works great.

- About proxies. Better than free or commercial sites, ask a friend who lives abroad to run a proxy for you. Keep this running as an emergency backup – "in case of revolution click here". I have a couple of proxies running for friends in different parts of the world for just that purpose.

> "- TrueCrypt. You already mention this, however you do not explicitly point out the single best feature of TrueCrypt compared to the many other disk encryption programs out there: plausible deniability. This feature allows you to have a hidden encrypted partition wihtin the encrypted partition. And there is no way an attacker can tell whether the second encrypted partition exists or not.
>
> http://www.truecrypt.org/docs/?s=plausible-deniability"
>
> TrueCrypt is great, but there is not much "plausible deniability" in practice.
>
> Just like its predecessor "Rubber Hose Cryptography", there is no way that you can ever satisfy the secret police torturers, that you really have given them all of the passphrases, to all of the hidden encrypted volumes.

Most modern computers with wireless capabilities have an option to change the MAC address. Changing this address routinely can make it more difficult to track and identify a specific computer system on a network.

Another use of this is to have mutiple people use the same MAC address, however you must insure they are never online at the time, also make sure most of them are using the network for purely 'legitamate' uses.

If you can use a MAC address from a source the regime trusts, you are less likely to be noticed as suspicious, and if packet inspection software does tag your use as suspicious, this creates suspicion and mistrust in the regimes ranks as they believe they have a 'mole'.

Speaking about destroying data on flash drives, smart cards, RFID chips etc. I'd try microwaving them for a while.

It's good for destroying CD/DVD too. The only caveat is that some devices may melt and/or produce noxious fumes, so I wouldn't use the same microwave for food without ventilating it and cleaning it up thoroughly. Also, the microwave itself may get eventually damaged if there's no water to absorb all the energy.

In an emergency situation I'd just throw all my solid state memory devices in the microwave, turn it on and run away.

EFF posted its own recommendations less than a month after yours came out. You are setting the agenda in the public square! http://www.eff.org/wp/surveillance-self-defense-international

Electronic Frontier Foundation is a leading American advocacy organization for digital rights and privacy, producing both publications and litigation in the public interest.

You deleted your cookies? Think again!

From Wired Magazine:

http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again/

Thanks for these security tips, especially on IP telephony.

Hi, nice article, here are some other information about .mov file extension. Nice day. Michal

Get flash sticks that don't look like flash sticks? I already lose one a month, now you want me to camouflage them? Also, I don't get the Skype fear. I just cannot see criminals listening to hours and hours of information on mp3 unless they KNOW that a certain call contains something. For the most part, your security should just be enough to keep you protected. Anyway, nice post. I have enjoyed the comments as much as the entry.

For blogging, you could try Baywords . For encrypted SMSes, use CryptoSMS: .

Baywords is run by the folks behind The Pirate Bay. They claim not to keep IP log details.

CryptoSMS takes a) compatible phone (of which there are many); b) patience. But it works.

Skype has a well known backdoor that is shared with law enforcement in many countries – http://www.h-online.com/security/news/item/Speculation-over-back-door-in-Skype-736607.html

There has been intense speculation, but no proof; the fact that Skype is allowed to operate commercially in countries that otherwise block VoIP should tell you something.

Also, while your guide is a good first step, the section on securing computers is a little impoverished, but unfortunately that's the lay of the land, for short of writing a book length introduction, there's not much that can be done.

P.S. Turn off wordpress snapshots on your site – it leaves cookies, and aggregates information – not a good idea.

The best free antivirus download is at ESET NOD32 Smart Security 4 and ESET NOD32 Antivirus4

Great info, some additional info on the .mov file extension here. Keep up the good work 

By the check out the Professional Training and Certifications for Ethical Hackers check this link: http://www.eccouncil.org/certification/certified_ethical_hacker.aspx

How about this one: never ever use a computer to communicate as it needs a network connection to do so, and any computer, connected to any network, it a complete security nightmare, always! Don't use it to encrypt stuff, don't use it to send stuff, don't use it to process sensitive data. This isn't paranoia, this is unfortunately reality in today's digital world. Bring me the first PC without any virus, malware or some unidentified running processes. The only secure PC is a stand alone PC without network card. It's ideal to encrypt and process your data, but if you send it afterwards with another PC, you will never be able to deny it.

Cipher Machines & Cryptology
http://users.telenet.be/d.rijmenants
http://rijmenants.blogspot.com

The complete guide to secure communications with the one-time pad cipher:

http://users.telenet.be/d.rijmenants/papers/one_time_pad.pdf