How to Communicate Securely in Repressive Environments

A Guide for Improving Digital Security - Updated June 28, 2009

This draft guide is intended for political activists operating in non-permissive environments and those supporting their efforts.

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 and/by imposing 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.

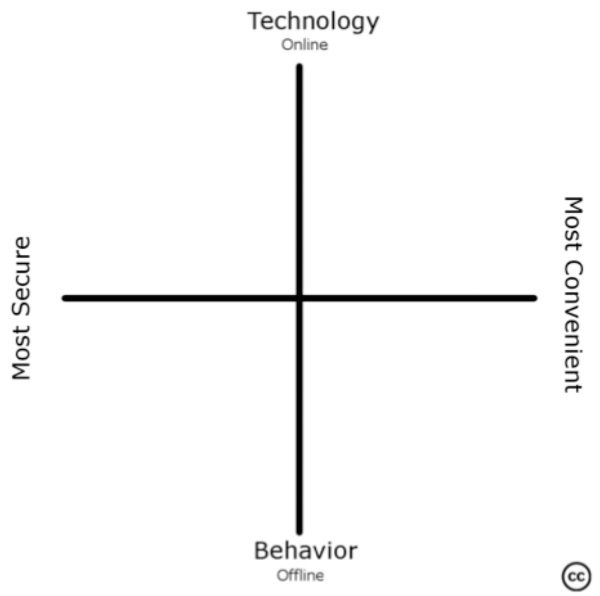
Adaptive Learning

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 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. Unlike the hierarchical, centralized structures of repressive regimes, networks have more flexibility and feedback loops, which make them more adaptable.

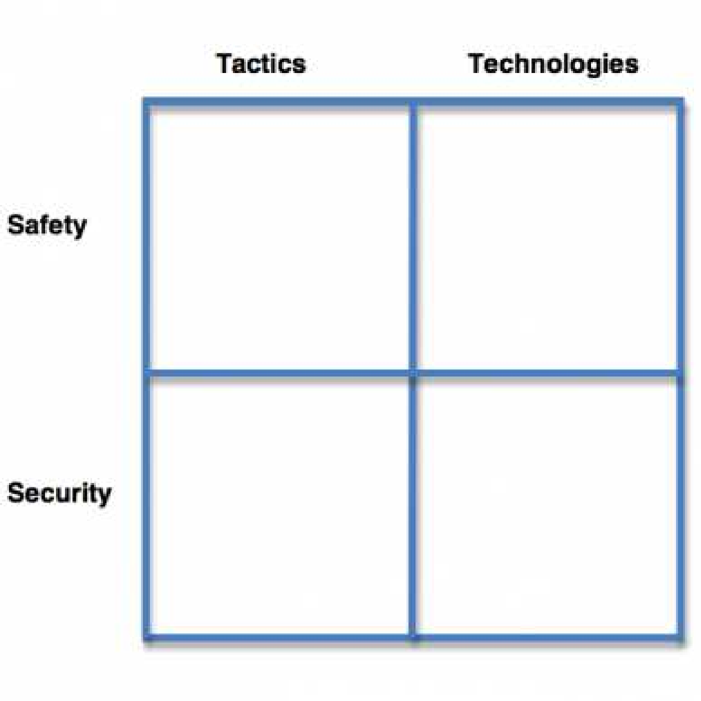
The normative motivation behind this research on digital resistance is based on the recognition by “many scholars and practitioners […] that the techniques associated with strategic nonviolent social movements are greatly **enhanced by access** to modern information communication technologies, such as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

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:



	Tactics	Technologies
Safety		
Security		

- **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. Furthermore, given the nature of technological change, some of the tactics and technologies below may no longer be effective in the near future. To this end, activists who follow the digital security tactics and technologies listed below should take care not to gain a **false sense of security**.

The digital security landscape is always evolving and the dynamic between digital activists and repressive regimes is akin to a **cyber game of cat-and-mouse**, albeit a dangerous zero-sum game. Finally, be aware that using more sophisticated tactics and technologies may call attention to yourself and label you as a serious threat. Please see the conclusion for a list of references 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.

- **Radios**

    - Radios can be used when cell/mobile phone networks have been shut down. Use code and never reveal your location. See also FreedomFone.
    - Radio broadcasts can be geo-located so do not broadcast at length from the same locations at the same times.
    - Ideally, use handheld radios and broadcast from a moving vehicle. This prevents you from being geo-located and allows you to broadcast over a wider area.
    - If you know your radio broadcasts are being interrupted (or voice call, SMS, emails, etc) you can deliberately produce disinformation and provide wrong information about meetings, protests, etc.

- **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. 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.
    - 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 reduce the 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 allegedly be turned into potential listening/tracking devices. Network operators may be able to remotely activate a phone as a recording device regardless of whether someone is using the phone or whether the phone 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.
  - Set a phone lock code to prevent others from quickly or easily accessing your phone.
  - 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.

- **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 passphrases for all your sensitive data, including your computer login account.
  - Keep your most sensitive files on flash disks and find safe places to hide them. Better yet, encrypt your data and make sure you have some only-slightly-sensitive encrypted data that you can “be forced to give up” in order to be credible when you deny the existence of your highly-sensitive encyrpted data.
  - Have a contingency plan to physically destroy or get rid of your computer at short notice. Know how to remove the hard drive from your computer to quickly hide or destory it to prevent most attempts to retrieve the data.

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

- **Email communication**
  - Use code if encryption is not possible.
  - Use passphrases instead of passwords and change them regularly. Use letters, numbers and other characters to make them “c0mpLeX!”. Do not use personal information and change your passphrases each month. Do not use the same password for multiple sites.
  - If you use Gmail and think someone knows your password, you can check to see if other users are looking in on your Gmail account. At the bottom of the Gmail email page, there is a statement that says "Last account activity: X hours ago on this computer. Details." Click on the "Details" link and you can see what IP addresses have recently accessed your account. If you see unusual IPs that are not yours, that may be an indication that someone else has entered your Gmail account. It is a good idea to do this every time you use Gmail.
  - Never use real names for email addresses but do 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 changes (see terms of service tracker).

- **Browsers and websites**
  - Turn off java, javascript, ActiveX and other potentially malicious features or add-ons.
  - Learn IP addresses of key 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.
  - Use Firefox but not Internet Explorer whenever possible.

- **VoIP**
  - Just because you’re talking online doesn’t mean you are not under surveillance.
  - As with a cell or landline, use code and 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.
  - How to post to Google Groups and send email anonymously using GPG encryption and anonymous remailer chains. 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. 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.

- **File sharing**
    - 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.
    - Carry as little as possible on you or a backpack with random, worthless items.
    - Assume computers at cyber cafes are tracking key strokes and capturing screenshots. If you are at an Internet café (or not using your own computer), then do not enter your password all at once. Keylogging hardware and software can track the keystrokes that you enter. But keylogging hardware and software captures ALL the keystrokes you make and does not know where you are typing it. So it your password is a8s$s1k&mz you can follow these steps. So if your password is "s9w1nn" then type "s" into the password box and then other nonsense keystrokes *outside* the password box into another window, eg "biteme". Then type "9" into the password box, and again nonsense keystroks *outside* the password box, etc.
    - Avoid cyber cafes without an easy exit and have a contingency plan if you need to leave rapidly.
    - Wear a double-sided jacket, a short t-shirt underneath a long shirt, etc, in order to change clothing easily after making a quick exit.

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.

- **Radios**

    - Radio jamming equipment are commercially available but keep in mind that they are illegal in certain countries.

- **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 micro (or mini) SD card with a mico SD-SD converter. Then place the micro SD into a compatible phone for safekeeping. Micro SD card readers are not much bigger than the card itself and can be practically hidden in plain sight. Here is an example.

- **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, along with Spybot Search & Destroy to remove threats spread by websites.
  - 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 and Windows users can use ZoneAlarm.
  - 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. For fast and secure wipe of the entire hard drive in case of an emergency try Darik’s “Boot And Nuke”.

- **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. Set this to be the default automatic option by visiting Settings: “Always use https”. Request that the individuals you send emails to via Gmail also use https. Do not open attachments, use “view” instead in Gmail to avoid downloading viruses.
  - Use encrypted email platforms such as Hushmail and RiseUp.
  - Use a PGP solution such Thunderbird’s Enigmail, Firefox’s FireGPG and GPG4Win.

- **Browsers and websites**

  - Use Firefox and get certain plugins to follow website tracking such as ghostery and adblock, adart to remove ads/trackers.
  - Use Tor software or Psiphon to browse privately and securely.
  - Use XeroBank browser, an anonymous browser designed to run on both Tor and XeroBank anonymity networks.
  - Always use *https* in “Settings/General/Browser Connection.”
  - Use browser proxy servers to browse anonymously and securely. Free browser proxies include *[names of proxies have been removed so they will not be identified and blocked by authorities]*
  - However, because these are free and popular, they are often slow and blocked by governments.
  - If you or a friend have a credit card or a PayPal account, you can use a for-fee (and thus faster, and also less likely to be blocked) browser proxy server such as *[names of proxies have been removed so they will not be identified and blocked by authorities]* for ~USD4/mo; some companies offer as a service regular updates to a list of proxy servers, and even software to manage such lists (such as ArchiCrypt and SwitchProxy).
  - Access points for secure browsers, Proxy servers and VPNs cannot be listed here for security reasons. Please get in touch to obtain a list.

- **VoIP**

  - Use Skype but not TOM Skype (Chinese version). Note that Skype is not 100% secure and has supposedly been compromised. There is no way to determine if a back-door has been written into the Skype protocol in order to (for example) comply with law-enforcement requests.
  - Off The Record (OTR) is a good encryption plugin. For example, use Pidgin with OTR (you need to add the plug-in yourself). Do *not* use Pidgin and OTR to transfer senstive files.
  - Gizmo offers 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 IM services.

- **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.
  - Use Crabgrass, which is designed by the Rise-Up Collective to provide a 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.

- **File sharing**

  - Use Skype to transfer files but *not Pidgin*.
  - 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.
  - Use Martus, an encrypted database software designed to keep sensitive data secure. This is considered one of the best tools for journalists, human rights workers to encrypt data.

- **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
- Frontline Defenders
- FreeBeagles;
- FLOSS Manuals;
- Feedback from DigiActive and Digital Democracy;
- Personal experience and that of other colleagues in the field.