Covert Communications

Disclaimer - Most of the info below has been "borrowed" from an American based website.

In a world where it is becoming increasingly difficult to keep secrets, learning how to communicate covertly is more important than ever. Whether you're trying to avoid detection by criminals, hackers, or the government, or you're an abused spouse hiding from an ex, but still want to be able to speak to your family or friend; specific communication methods are more secure and less likely to be intercepted. We will explore some of the most popular covert communication methods and discuss how you can use them yourself. These techniques would also come in handy if the SHTF. Stay safe and concealed!
Covert communications is for everyone who understands that the surveillance state is out of control.
Since most of us will not be able to utilize encrypted radio over satellite with our own special equipment and satellites, we're going to talk about lower-tech options. Identifying covert communications using forensic analysis and everyday investigative methods is easier than one might think, so you must be incredibly careful.

Burner Phones

There is a lot of misinformation about burner phones and how they can be used. The truth: these devices aren't as untraceable or easy to use when we think about them in terms of privacy concerns, but here are some key tips to ensure you're being safe when using one:
1.Don't buy your burner phones online or in a big box-type store. Always pick up your burner phone in a convenience store outside of your hometown.
2.Do not buy a "smartphone" as a burner. Stick with a non-smartphone version.
3.Never use "burner phone numbers" that you can get through an app on your actual phone.
4.Never keep your burner phone and your regular phone together if the burner phone is on. Anyone looking at cell or tower records can get an idea that the same person owns those two phones. Try to never carry the burner when you have your personal phone on, and NEVER turn on the burner at your house or in your neighborhood.
5.Change burner phone providers often (if you're using it a lot) and randomize usage habits, including locations, often.
6.Before you sign up for any service, it's important that the terms and privacy policies are clear. Be sure to review them carefully so there aren't surprises later on down the road! Obviously, don't use your real name or info.

7.Always pay cash and do not get a receipt. Do not even touch the receipt, have the clerk throw it away.
8.Purchase pre-paid only, no plans.
9.Activate the phone and SIM a few days after you get it, in a densely populated residential area nowhere near yours, preferably at a large apartment complex. Always leave the default voicemail.
10.Never send texts with private info from the burner.
11.Never use your burner phone near your neighborhood.

Break Phone Setup

1.Purchase 3 burner phones.
2.Give one of them to your contact.
3.Take the second burner and set up call forwarding to your contact's phone.
4.Save the number to the second phone, and then destroy it completely.
5.Call the broken phone to call your contact. This way if your contacts phone becomes compromised, the call will be traced to the broken phone, not to you. If you're using and randomizing burner phones using the techniques described in the last section, you should be nearly impossible to trace.
6.You can use a 4th phone for covert communications in the other direction as well.

What about anonymous apps like Signal?

If you're well versed on how to safely use a "smartphone" version of a burner, which is still not recommended, coded conversations using applications like Telegram, Signal, WhatsApp, and other secure messaging apps are the new way to stay in touch with friends. They offer an additional layer of protection for your messages that goes beyond just being able to communicate privately – it's also anonymous and encrypted. Signal is also recommended by Edward Snowden, who knows a thing or two about communications.
These features make VOIP calling (Voice over internet protocol (VoIP) is a type of phone system that uses an internet connection to make and receive calls, rather than traditional landlines) even easier than ever before; you can call anyone who has either app without worrying about whether or not they'll see what was sent to you next time around (because deleting each conversation from both participants will get rid of any trace)
Texting and calling apps are traceable if you use them incorrectly. So when should we be worried about being traced while using anonymous text messages? If your voice or photographs get added to the message because of features like facial recognition, then that's one-way data can link back to our real-life identities. Do not leave a trail outside of your app by calling/sending messages through it on a phone line that will link back to YOU, and do not forward calls or send messages

from the app to your actual number. Keep your covert communications just that, covert!

What about using email?

If we learned one thing from Hillary Clinton about covert communications, it's that we need to be really careful what we're sending out via email. Looking for an uncomplicated way to communicate covertly via email?

1.Setup up one random email account
2.Share the login with your contact covertly, in person if possible
3.Log in and start drafting an email but don't send it. Save it as a draft
4.Have your contact go in and open the draft and respond to you; still never actually send the email
5.You're going to want to use Proton Mail or another service that DOES NOT save draft emails or any emails on their server.

If you want to avoid internet or phone communication totally what other options are there?

UHF/CB radios – The 2 main problems are range (usually line of sight) and security of messages. Anyone with a UHF tranceiver or scanner can listen in, so pre-arranged code words or phrases would be a way to maintain secrecy.

Letters – using the NZ mail service – in theory this is private, but realistically mail can be opened, read and resealed.
An option could be to write in invisible ink. It's an ancient method, but still a very effective one. What you do is write a convincing, but harmless, letter that doesn't reveal anything important. Then you use the remaining space on the page to write another, secret, message that won't show up unless someone knows how to reveal it. Modern invisible ink usually glows under an ultraviolet light, but most people don't have an ultraviolet light handy.
Luckily there are older ways to make invisible ink, and they still work very well. Centuries ago a solution of ferrous sulfate was used as an invisible ink. A message could be written with it, and would disappear completely when dry. However, when the paper was heated the message would reappear. If you don't have any ferrous sulfate handy you can get exactly the same effect with lemon juice. The only problem with that is that the letter will smell of lemons for a while after the message is written, and someone might guess what you've done. If you can, leave it for a while to let the smell fade before you put it in an envelope and send it. Messages written with these inks don't need a lot of heat to reveal them. There's no danger of the hidden writing appearing from someone's body heat, but you don't need to risk setting fire to them either. Holding it close to a light bulb will usually be enough. There's another way to hide a message in a letter without using

invisible ink, but it needs a bit more preparation and you have to use some artistry to pull it off, but if it works it's very effective. It's called a mask letter. To write a mask letter you need a mask – a sheet of paper the same size as your notepaper, with blocks cut out of it in a random pattern. To write a message, you put the mask on top of a sheet of paper and write the message in the blocks. Then you take the mask off and compose a normal, innocent letter around the secret one. When the letter gets to the other end, all the receiver has to do is put their own mask over it and the hidden message will appear. Obviously there's a potential weakness here – sender and receiver both need to have a copy of the mask. This isn't a method you can use without preparing in advance. If you have prepared however, it's very effective. Cops and anyone who knows something about secret writing will routinely heat up any letters they're suspicious of, just to see if invisible ink has been used. They might also use UV and chemicals. A well-written mask letter, however, is immune to all of these tricks.

Use a dead drop – using a predetermined hiding place to leave messages (or other items) to be collected by your contact. It would be wise to have several dead drop options using the P.A.C.E. System (Primary, Alternative, Contingency, Emergency).

Talk to people in person, away from any/all electronic devices. Old school pre-digital era in-person signaling and drops are still best.