Old-school Low-tech Covert Comms

Do you have a plan to communicate securely over insecure methods? Low-tech methods can be used to relay and receive messages without them being understood by others who are watching, listening, or reading and they might be more relevant than ever as the recent mobile network outages throughout the US showed us.

Low-tech Tradecraft Techniques

Low-tech tradecraft techniques have been proven to work even against high tech adversaries.

Communications Plan

In its simplest form, a radio communications plan is simple two people with radios agreeing that they will listen for each other on a particular frequency at a given time and date, such as 22:00-22:15 every Friday. Communications plans can use different media and added complexity to make the message unintelligible to anyone other than the intended recipient.

Couriers and Cutouts

The raid that killed bin Laden also captured hundreds of gigabytes of data on hard drives, in excess of 100 USB memory sticks, media from a video camera, in a process known as sensitive site exploitation. They even got his journal.

A couple hundred gigabytes of this information was released in 2017 and it reveals some of the tradecraft he used to evade the most powerful nations on Earth for nearly a decade, including his well-reasoned argument for sticking to old-school, low-tech tradecraft instead of relying on constantly changing technology.

While I am certainly no fan of his, it was nevertheless a remarkable achievement to evade the U.S. and her allies for a humiliatingly long ten-and-a-half years. I have researched the stories of many fugitives over more than a decade, and few fugitives have evaded the most powerful nations on the planet for over a decade post-2000. The guy grew old and grey, and darn near died of old age before they found him, and they very nearly didn't find him at all. To top it off, he did it with wives, kids, grandkids, and two bodyguards in tow … around 20 people in all.

Plenty of voices claimed, "bin Laden was able to hide in that compound because Pakistani military intelligence was helping him." And it might be naïve to take the position that no he received no aid whatsoever from anyone in the Pakistani government … perhaps almost as naïve as to believe that the U.S. and her allies didn't have their own sources in the Pakistani government who would have tipped them off to the fact if he was receiving aid from the Pakistani government itself.

Whether the Pakistani government aided him or not, bin Laden stayed hidden from the U.S. largely by compartmenting his identity, his household, and his communications and by using trusted couriers instead of email, and by disciplined enforcement of his household security SOP.

He closed his compound off from the outside world. They had a garden, chickens, and milk cow for food. Children weren't allowed outside without an adult to control the noise. They burned their trash. The compound had no phone or internet connection. TV reception was via satellite receiver. They homeschooled the kids who were only allowed to leave the compound “except for urgent necessities such as medical treatment.”

Analysts look at the home movies and see a paranoid old man living in squalor. I see an extremist living in a largely self-contained survival retreat, hiding in plain sight.

To send emails, he would write his message on an air gapped computer (not connected to a network), saved it to a flash drive. A trusted courier would pick up the flash drive and send the message from an internet café.

Politicians and bureaucrats wanting to restrict encryption alleged that bin Laden was a master of encryption and that’s why message scrambling technology must be banned. “The world should be less free because of fear! Terrorism! Quick, give up your rights to privacy and everything else!”

Politicians convinced simple, cowardly voters to do what bin Laden never could have done … make America less free … and so made bin Laden’s victory more complete than he could have hoped.

Contrary to what the politicians, FBI Director Freeh, and their media fearmongers had been telling us, bin Laden thought that using encrypted email was nuts. When his chief of staff tried to convince him to use email because it was so difficult to use couriers, he responded, “I think that sending anything confidential and dangerous through email dependent on encryption is a risk.” “Communications should only be through couriers to relay the message to the appropriate party.” (Geographic, 2022)

Duress Signal

If someone puts a gun to your head and dials a family member, do you have a way to warn them that you are being coerced? Shared in advance as a duress signal, a harmless phrase can be used to alert them. “I love you honey” works if your wife hates being called “honey.” Telling a family member to, “Tell spot to be quiet.” works if Spot is long dead and your new dog is named “Yeller.”

If coerced to sign a document, adding the abbreviation for “vi coactus” to your name (V.C.), which is Latin for “having been forced” or “having been coerced”, is a customary signal. (Wikipedia, Vi coactus, 2024)

Numbered Messages

Do you have a way to relay information about people, status, needs, and places to people you trust over phone lines, the postal system, or email? A system of numbered messages most people are probably familiar with is the 10-code system used over the radio by law enforcement. 10-code systems typically offer little security because anyone can look them up, but numbered messages are secure if the system is not known by the listener.

Truchet Tiles

Sometimes is desirable to communicate a message visually as Admiral Jeramiah Denton famously blinked the word “TORTURE” in Morse code during a propaganda TV broadcast (as a Commander) during the Vietnam War. Covert visual communications could get your message out in a kangaroo court, propaganda video, proof of life video, perp walk, or any other video or photo made under duress.

Truchet tiles can simplify the process by giving you the ability to visually communicate codes or numbered messages. A Truchet tile is a square tile that is not rotationally symmetric, therefore each tile has four possible orientations. Each orientation can be assigned a numerical value or meaning, as is done in binary code, only each digit has 4 possibilities instead of just 2.

Six 1” tiles fit in the space of a Velcro flag patch, so such a space can be used to visually communicate a few numbered messages or codes with what looks like harmless art. (Wikipedia, Truchet tiles, 2023) The tiles can be made from duct tape and IFF squares or any small rotationally symmetrical tiles that fit in the loop field.

SARNEG, SARDOT, and Code Words

Chapter 14 – Evasion & Survival, Section-5 Communications in the Ranger Handbook has a few paragraphs on choosing a SARNEG, SARDOT, and code words. (Army, 2011)

SARNEG stands for Search & Rescue Numeric Encryption Grid. A numeric encryption grid is simply 10-letter word with no repeating letters such as “palindrome”, “blackhorse”, or “silverback”. Because they have ten letters that do not repeat, the letters can be substituted for numbers 0-9 as a simple substitution cipher enabling numbers to be passed over insecure communications channels such as unencrypted or compromised radio.

SARDOT stands for Search & Rescue Dot, as in a dot on the map or geographic location. The SARDOT can be used to communicate anyplace else on the map by giving the bearing and distance from the SARDOT, both of which are scrambled using the SARNEG.

Code words are like numbered messages only they substitute a word for a meaning rather than number, which has the advantage of being easier to remember. Many survivalists will recall the use of code words over the radio in the original Red Dawn movie, “The chair is against the wall” … and “John has a long mustache.”

Survival instructor once David Holladay suggested using names for code words. If I use the name “Roy”, I could be referring some guy name Roy, or Roy Utah, or Roy, Idaho, or I could be referring to some rock we named Roy. Using names as code words also makes them easy to work into normal conversation.

Using a SARNEG, SARDOT, or codewords are not super secure by themselves, but by using them together the information will usually be useless in an E&E scenario where the target is on the move. If additional layers of security are added, it may never be cracked.

OTP Encryption

One-time pad encryption is a simple encryption system that cannot be cracked as long as:

- The key is as long or longer than the plaintext.
- The key is truly random.
- The key (or any part thereof) is never reused.
- The key is kept secret by those using it.

Identical pads of paper with serialized sheets were used. Once a key was used, that sheet was burned. Pads were sometimes treated with nitrocellulose so they would burn quickly, completely and leave no ash. The treatment process is simple and can be performed at home. I wouldn’t take a pad so treated through airport security though.

Let’s say Bonnie and Clyde want to use OTP. They create identical, random pads long enough for their messages and keep them secret and determine the order in which the pages will be used. They select a dead drop and signals to check it for an encrypted message.

Bonnie wants to send the message “exfil” to Clyde. If they assign each letter a number, a=0, b=1, c=2, d=3, e=4, f=5, g=6, h=7, i=8 and so on, and the OTP sheet begins PVKCH, the coding would be:

e x f i l
message

4 (e) 23 (x) 5 (f) 8 (i) 11 (l) message

+ 15 (P) 21 (V) 10 (K) 2 (C) 7 (H) key

= 19 44 15 10 18 message + key

= 19 (T) 18 (S) 15 (P) 10 (K) 18 (S) message + key mod 26

T S P K S
ciphertext

If the value is greater than 25, such as happened with the second letter, then 26 is subtracted as in modular arithmetic, so if we get a number that surpasses “Z” we start over at “A”.

Therefore, the message Bonnie sends to Clyde is “TSPKS”.

Clyde then decodes the message by subtracting the key from the ciphertext:

T S P K S
ciphertext

19 (T) 18 (S) 15 (P) 10 (K) 18 (S) ciphertext

– 15 (P) 21 (V) 10 (K) 2 (C) 7 (H) key

– 4 -3 5 8 11
ciphertext – key

= 4 (e) 23 (x) 5 (f) 8 (i) 11 (l) ciphertext – key mod 26

e x f i l

message

If a negative number is generated, such as happened with the second letter, then 26 is added to arrive at a number equal to or greater than 0.

Therefore, Clyde uses the key from his OTP to decipher Bonnie’s message to him of “exfil”. (Wikipedia, One-time pad, 2024)

CLICK HERE <<
TO CLAIM YOUR COPY OF 'BLAST PROOF' AND FIND OUT HOW TO SURVIVE WHEN THE LIGHTS GO OUT
BLAST PROOF

One-way Numeric Pagers

One-way pagers receive numeric messages. They don’t send signals, so they can’t be traced. So long as the users are insulated from the purchase of the pagers and payment of service by a cutout they cannot be traced and are a way to receive numbered messages without compromising your location. Service area for the transmitter is usually a metropolitan area.

Faraday Bag

An IT forensics bag or RF shielded pocket liner functions as a shielded envelope to attenuate RF signals to the point where a cellphone placed in the shielded envelope is unable to communicate with Wi-Fi or cell towers.

IT forensics people use them because no one can communicate with the cellphone to initiate a remote wipe while it is in the bag. Survivalist like them because the phone is provided some (usually around 75dB) of shielding against HEMP. Cellphones, passports, ID, and bank cards carried in a pocket liner also cannot be hacked, tracked, or skimmed while inside the liner, making them a must-have for international travel or anyone who doesn’t enjoy being constantly tracked or anyone averse to leaving giant mountains of evidence for overzealous law enforcement, prosecutors, or ambulance chasers to dig through to cherry-pick bits of evidence they can present in a context that fits the narrative they are motivated to sell.

References

Army, U. (2011). Evasion & Survival – Communications. In U. Army, *Ranger Handbook* (pp. 14-5). Fort Benning, GA: U.S. Army.

Geographic, N. (2022, March 26). *Bin Laden’s Hard Drive*. Retrieved from YouTube: https://youtu.be/4W_P_Yxhnt0?si=V8yjhhsDjf-pU-Fp

Wikipedia. (2023, November 16). *Truchet tiles*. Retrieved from www.wikipedia.org: https://en.wikipedia.org/wiki/Truchet_tiles

Wikipedia. (2024, February 24). *One-time pad*. Retrieved from www.wikipedia.org: https://en.wikipedia.org/wiki/One-time_pad

Wikipedia. (2024, January 29). *Vi coactus*. Retrieved from www.wikipedia.org: https://en.wikipedia.org/wiki/Vi_coactus