Christians Behind Enemy Lines
How High & Low-Tech Tools and Methods
Can Help Pastors and Non-Pastors

For pastors, there are two primary options for the survival of an uncompromising church behind enemy lines.

Option 1: Remain a surface-level (publicly visible) brick and mortar church, but in the USA mitigate the risks by becoming a 508(c)(1)(A), and implement some modern anti-censorship tools.

Option 2: Become an underground church, Internet-based church, or home-fellowship utilizing ancient and modern methods to remain operational.

This document will explore some of the tools and methods for option number two, most of which also apply to surface-level churches and individuals.

Digital strategies for communication behind enemy lines:

1. If possible, do not use Microsoft, Apple, or Google-based devices for communication, which includes cellphones. Instead, use open-source Linux-based desktop[1]/laptop[2] computers with a secure operating system,[3] mini-Linux computers,[4, 5] and Linux open-source cellphones.[6, 7]
2. Do not use Microsoft, Apple, or Google-based office software. Instead, use LibreOffice or OpenOffice.
3. Do not use Microsoft, Apple, Google, or Yahoo for email. Instead, use free private encrypted email like Protonmail (based in Switzerland), Mailfence (based in Belgium), or Tutanota (based in Germany). You may want a free account for all three to maximize redundancy.
4. Store your church documents and other files across multiple encrypted storage platforms, spanning different countries if possible. See these examples: Mega.nz, pCloud.com, MediaFire.com, and Archive.org.
5. Using a secure encrypted connection out to the Internet can help bypass censorship, and as such we recommend using one or more Virtual Private Networks (VPNs).[8]
6. If you operate a website, consider obtaining a failover hosting provider in an anti-censorship country, such as Sweden. Your website should be designed so that it is not dependent on WordPress, etc. and instead it should be self-contained, which will make it easy to move at a moment's notice to any hosting provider that exists in the world. There is useful information on setting this up from Arcana-X, and they also offer a good example of how to diversify your website across multiple technologies. [9, 10, 11, 12] You should also consider archiving your website for free by going to Archive.org/web. You can see a version of our site archived by clicking the following link: TheTorchbearerSeries.com. Do not rely on only one source or method.
7. You can send messages encoded into images, called Image Steganography, by using an online service like the one that PELock provides.
8. Another method to safeguard biblical documents, and/or communicated information, is to use encrypted BitTorrents. Torrents should be used with a VPN to stay more anonymous in conjunction with a good open-source software client, such as qBittorrent, then connect to a large BitTorrent network, such as The Pirate Bay. See How to Use BitTorrent for more information. The distributed peer-to-peer (PTP) BitTorrent network is similar to the IPFS network. Note: If you use Adobe Reader to view PDF documents, make sure you turn off Java within it by going to *Edit > Preferences > JavaScript* and then uncheck the box *"Enable Acrobat JavaScript"*. This will prevent malicious PDFs from executing.

Physical strategies for communication behind enemy lines:

1. Many underground churches will have members meet at each other's houses, but this is not always the best idea, since some neighbors will get nosey if there are people over on the same day of the week. Another option can be to meet at a park or cemetery, or drive in a car and discuss the Bible while driving.
2. Avoid physically meeting and driving in areas that have surveillance cameras outside if possible, since many can track license plates, have facial recognition, and even reconstruct a conversation if it can see mouth movement (lip reading).[13, 14]
3. Do not travel to Bible meetings with your cellphone, and do not speak about important biblical subjects with a cellphone in the same room, even if you think it is powered off. It has been demonstrated that cellphones can track a person's location and record conversations while 'powered off'[15] or track a person with location services off[16] or with no sim card installed with airplane mode on.[17] The only way to ensure a phone is truly powered completely off is to remove the battery, so it is often better to leave it behind.
4. A single-use paper cipher could also be useful depending on how dangerous the country is, which could also be used through email. Using the below example, that both parties would have, the code *A5B1A4B3A3B4A3B3A2B1* is decoded as *TODAY*. Never reuse the same row and column more than one time, which will ensure that the resulting code has zero repeating patterns and thus unbreakable without the key. To make the code more obscure, the code can be hidden in an encrypted image like the previously mentioned PELock, or the rows and columns can use symbols instead of letter/number combinations. Avoid using any multi-use ciphers, which are easily decrypted with a computer (i.e., a paper cipher wheel).[18]
5. When a Bible group reaches twelve members, it could split into two groups and also break off all prior communication with the original parent group. This compartmentalizes the groups and minimizes the risk to all the groups if in the event a single group is compromised by a member.

SIMPLE EXAMPLE CIPHER USING ROWS AND COLUMNS							
	A1	A2	A3	A4	A5	A6	etc.
B1	E	Y	X	B	T	G	C
B2	J	P	J	E	C	J	S
B3	K	S	A	O	F	Z	D
B4	Q	R	D	N	H	R	S
B5	L	U	B	X	I	E	B
B6	V	D	M	W	O	A	L
etc.	D	I	W	O	C	K	E

SIMPLE EXAMPLE CIPHER USING ASCII SYMBOLS							
	⋔	℀	↕	φ	Ɜ	ꛤ	etc.
Ɀ	E	Y	X	B	T	G	C
฿	J	P	J	E	C	J	S
◯	K	S	A	O	F	Z	D
ὼ	Q	R	D	N	H	R	S
†	L	U	B	X	I	E	B
Ꙇ	V	D	M	W	O	A	L
etc.	D	I	W	O	C	K	E

Old Testament: *"Let us hear the conclusion of the whole matter: Fear God, and keep his commandments: for this is the whole duty of man."* – Ecclesiastes 12:13 (KJV)

New Testament: God said, *"If ye love me, keep my commandments."* – John 14:15 (KJV)

Bibliography

[1] Think Penguin Staff. "The Penguin Pro 11 GNU / Linux Desktop" *Think Penguin*. March, 2021. (Cost around $550+)

[2] Purism Staff. "The Road Warrior Laptop" *Puri.sm*. March, 2021. (One of the most secure/private laptops $1,470)

[3] Ray Walsh. "Which Linux distro is best for privacy?" *ProPrivacy.com*. July, 2020. (Free software)

[4] Arcana-X Staff. "Arcana-X Freedom Box" *Arcana-X.com*. March, 2021. (Easy DIY for around $150)

[5] Purism Staff. "Purism Mini" *Puri.sm*. March, 2021. (Cost around $700)

[6] Purism Staff. "Purism Librem 5 Cellphone" *Puri.sm*. March, 2021. (Cost around $700)

[7] Pine64 Staff. "Pine Phone Beta" *Pine Store*. March, 2021. (Cost around $200)

[8] Tom Spark. "VPN Tier List and Reviews" *VPN Tier List*. March, 2021.

[9] Arcana-X Site 1: http://www.arcana-x.com/

[10] Arcana-X Site 2: https://arcanax.ablative.website/

[11] Arcana-X Site 3: http://arcana-x.crypto/

[12] Arcana-X Site 4: http://s325e7vlska2z2f34fs3tgrusfwyuepk7reausby6ruhupkob2jqluad.onion/

[13] Security Today Staff. "Lip-reading technology breakthrough to be used on CCTV" *Security Today*. April, 2016.

[14] Jamie Condliffe. "AI Has Beaten Humans at Lip-reading" *MIT Technology Review* November, 2016.

[15] Raju PP. "Can You Track Switched Off Phones? Apparently, NSA Can!" *Technology Personalized*. February, 2021.

[16] Jennifer Schlesinger and Andrea Day. "How GPS can track you, even when you turn it off" *CNBC*. July, 2018.

[17] Tucker Carlson and Brett Larson. "How much info is Google getting from your phone?" *FOX News Channel*. February, 2018.

[18] Anonymous. "Making Paper Cryptography Tools" *Invent with Python*. March, 2021.