SECURITY

A RESISTANCE MANUAL

SAM CULPER

SECURITY

A RESISTANCE MANUAL

TABLE OF CONTENTS

ABOUT THE AUTHOR

Samuel Culper is a former military intelligence professional, and contractor for a United States Government intelligence program. The bulk of Sam's operational experience comes from working missions ranging from All-Source and Human Intelligence to Special Projects, biometrics, targeting, and senior-level advising; including multiple deployments to Iraq and Afghanistan. Sam left his stateside desk job a couple years ago to pursue other goals.

I owe a great deal of thanks to the Mountain Guerrilla, and to Western Rifle Shooters Association, for adding fuel to the torch of Liberty. These individuals introduced me to the resistance movement, and have provided ample support and encouragement to others and myself.

PREFACE

"**Be not intimidated, therefore, by any terrors… nor suffer yourselves to be wheedled out of your liberty...**" – John Adams in A Dissertation on the Canon and Feudal Law, 1765

We as a nation have failed to heed and *live out* the words and warnings of our Founders. We have been tricked, we've been bullied, and we've been force fed. Readers of the Free Forces blogoshphere and the Three Percent movement are today's rare exception. These Patriots will restore Liberty within our lifetimes.

The past decade has laid bare in all their ugliness repeated incursions into citizen privacy and new interpretations of the Fourth Amendment, the hyper-militarization of police, politicians operating under the table and above the law, skyrocketing national debt against the will of the People, and seemingly endless wars and conflict.

The time for defending domestic spying, rationalizing the police state, or justifying continued violations of the Bill of Rights has ended. It should not have started in the first place. We ought to realize that the regime is already preparing itself, and we ought to focus on solutions to preserve the flame of Liberty. What's the best we can hope for, and what's the best we can achieve?

The best we can do is to restore America regionally – perhaps portions of the South or the Mountain West. (I'm a particular proponent of Rawles's

American Redoubt.) Short of carving out and protecting a chunk of land where the ideals of American Liberty are defended and upheld, the best we can do is make the statists pay for their tyranny.

These solutions aren't popular, and they won't be achieved without some pain and sacrifice. Patriots enjoy citing Thomas Jefferson's oft-quoted words on the Tree of Liberty with regards to the blood of tyrants, but Jefferson also makes mention of the blood of patriots.

This ebook was written specifically for the Three Percent and resistance movements in order to provide a basic understanding of security measures each team, cell, militia, or other organization should take to make itself more secure and to prevent regime violence against it. Security of communications, information, personnel, and operations should absolutely be your top concern.

But security is a double-edge sword. In conflict, every strength is also a weakness. The greater your organization's security, the less efficient it will be. The more resources you dedicate to providing security, the fewer resources you'll have for offensive operations. The larger the adversary, the slower it becomes. The lighter it is, the less area it can actively hold. Resources are finite, force multipliers and unmanned systems included, even for potential adversaries.

Passive collection tools like NSA's XKeyscore and PRISM, on the other hand, will always be on and virtually everywhere. But even their strength of collection produces a weakness in that they can't triage and analyze every piece of collected information. There aren't enough regime analysts (made weaker by lack of skills), and computers simply aren't smart enough; programs are no replacement for human brains.

The regime will collect, regardless of their ability to process, so your mission as a resistance element is to survive in the gaps. The regime collection capability is an enduring threat, so developing a security-centric mindset and strategy is incumbent on you. Practice the security measures described, and hide your footprints. Make the regime analyst utilize his precious resources to find you in his haystack. No matter how vast his net, and no matter how deep his pockets, the regime analyst will always hurt for manpower, brainpower, and collection assets. You can't stop him from searching, but you can hide. In striking a balance between resources and security, we must answer how good is good enough?

CHAPTER ONE

COMMUNICATIONS SECURITY

Poor Communications Security (COMSEC) will lead to mission failure. Mission failure may come as the result of interception of all communications, or the discovery of one piece of information that allows the regime analyst to complete his understanding of your organization. The regime analyst may not need every piece of your puzzle to get a good view of the final image. In the eyes of the regime analyst, your organization is a puzzle waiting to be put together so treat every piece of information as if it's his last clue. What we say, when we say it, and where we say it matters.

COMSEC is a trade-off for time and efficiency. The concept of layering security measures is critically important, and we want to put as many security layers as necessary between the adversary and us. It will, however, affect the extent of our efforts, and the timeliness and efficiency of our communications. You can have perfect encryption but the encryption key then becomes as important as what you're encrypting. You may have flawless tradecraft but a mistake made by a counterpart could compromise you. You can send a courier with an encrypted message but it could be lost in transit, or it may take a week to receive a reply.

A recurring theme in all of security is risk. We ask ourselves questions like, "What risk does this piece of information pose to my organization?" A shopping list might present a low risk, whereas a list of personnel is high-risk information. Every time we communicate information electronically, we justify the importance of the message based on the risk of its interception. Yes, the need that this reaches its intended recipients justifies the risk of its potential discovery. If the importance of the communication doesn't justify the risk of sending it, then think twice about communicating your message electronically. And never communicate sensitive information through unsecured channels.

The prolific use of spying tools puts at risk all electronic communication. No phone conversation is safe. No email is safe. No internet traffic is safe. Always consider that what you transmit electronically is or can be made publicly available, along with the origin of the information. A first step to secure electronic communication is to get away from the free email services that actively access your data (Gmail, Yahoo, Hotmail, etc.), and move to more secure services (Hushmail, Enigmail, etc.). Even these, however, are not safe in and of themselves.

There's no doubt that an encrypted message is safer than plaintext. While encrypted email provides the ability to communicate securely across large distances, its weakness is that the discovery of your private encryption key or the physical confiscation of your computing hardware will void that layer of security. The bottom line is that encrypted communication is only as safe as you make it.

On the other hand, much of short distance communication can be achieved through couriers. Coded messages can be carried from cell to cell, or to and from the leadership element. This communication is safe from the regime insofar as it cannot be electronically collected, however it's still vulnerable to physical collection by regime checkpoints or other security elements. You will always trade efficiency in exchange for an added layer of security.

ENCRYPTION.

KEY. A key is a password or passphrase used to encrypt and decrypt messages and other information. A key can be a number, a word, a phrase, or a combination of letters, numbers, or symbols.

KEY PAIR. A key pair refers to asymmetric encryption, whereby a public key and private key are created and specifically linked to each other.

Symmetric encryption.

Many people are familiar with what cryptologists call "symmetric encryption" (also known as private key encryption), where the same key is used to encrypt and decrypt a message. In these systems, the secrecy and strength of they key is most important. If a key becomes compromised – that is, discovered by an adversary – then all communication encrypted by that key could be compromised. It's incredibly problematic. Although compromise is a critical security issue, symmetric encryption is much more efficient with regard to key management.

Key management is your distribution plan for keys. Will you opt for the most efficient manner and distribute your private key to all members of your cell, or will you create a separate private key for each individual? In the event that your cell shares the same key, any individual is then a linchpin in the undoing of your secure communications. If one member is comprised then you all may be. On the other hand, while the creation of multiple private keys will add a layer of security called compartmentalization – putting your eggs in different baskets, for instance – you will sacrifice efficiency in the flow of information. You may receive a message using one key, and then need to distribute that message to the rest of your organization using a handful of other, separate private keys.

Compromise is the worst possible thing that can happen to a resistance organization. You need to have a contingency plan in the event that a key is compromised. Will your counterparts alert you, or will you continue to converse unknowingly with the regime analyst? Formulate a plan with your team, and identify how you will alert any possible compromise. It's much better to be safe than sorry. If you use a coded message (covered later in this chapter) to alert a possible compromise, how will you distribute the new private key? You may choose to distribute new key information every couple weeks or months, you may develop a deliberate backup key to be used when the current channel is called into question, you may develop one group-wide key and multiple separate keys for more sensitive information, or you may utilize an identification and authorization passphrase (covered later in this chapter). Each contingency plan will bring with it new security challenges. You will always be trading efficiency to gain security.

PRO:
- Efficient method for small group communication.

CON:
- Best only when the key is agreed upon by sender and recipients face to face (not electronically).
- The more individuals who know the key, the more vulnerable the key is to compromise.
- There is no customer service to reset your key if you forget it.
- Your secret key is only as secure as you make it.
- Although the contents of your encrypted email may be safe, you may rouse suspicion from regime elements.

Asymmetric encryption.

Asymmetric encryption, also known as public key encryption, uses two keys; one to encrypt information, and another to decrypt information.

Your first key is a 'public key'. The public key is not secret; we went this key to be available to anyone who wants to send us a message. This greatly simplifies the problem of key distribution because we can broadcast a public key without worrying that it will be compromised. One of the simplest ways to do this is by publishing your key on a key server. However you make this key public, whether through email, key server, or hand off, information encrypted with your public key can only be decrypted with your matching private key.

Your private key belongs to you, and it must remain secret. Keep in mind that if your private key is compromised, then those who have access to your computer or have access to the encrypted emails will be able to decrypt the messages. Keeping your private key and hardware safe is critical. There are a couple things you can do when creating a private key that will improve its security.

- Set a key expiration, which tells others to stop using a public key after a certain date. The shorter the length of time a key is valid, the less damage a stolen key can do.
- Set a passphrase so that if your private key is compromised, others cannot intercept messages to you, or impersonate you.

The asymmetric encryption process works in reverse when sending encrypted information. You will utilize others' public keys to encrypt information, and the recipients will utilize their private keys to decrypt your message. In an encrypted conversation through email, the sender will always utilize the recipient's public key.

The private key can also be used to digitally sign a message (which doesn't encrypt it). The digital signature can then be validated by anyone who possesses the public key. Digital signing is an important tool in larger networks, or when the message's veracity may be called into question. It's one way to verify that the sender is who he says he is. Unless you are very strictly following key expiration protocols, signing your messages may not be in your best interest. Anything you digitally sign, you now own, especially in the court of law.

PRO:
- Allows you to receive encrypted information without distributing a secret key.
- More secure because your secret key is private.

CON:
- There is no customer service to reset your key if you forget it.
- Your private key is only as secure as you make it, and is made vulnerable through coercion.
- Although the contents of your encrypted email may be safe, you may rouse suspicion from regime elements.

End-to-end encryption is vitally important. Information transits the Internet completely unsecured unless you secure it at the endpoints. You must be doing the encryption on a machine that you can physically touch - even better if it is a trusted operating system (such as TAILS).

Once we've encrypted our communications, we should start thinking about traffic analysis in the backdrop of Signals Intelligence (SIGINT) – that is, avoiding the leakage of information even when encryption tradecraft is perfect. Recent revelations about regime SIGINT programs like XKeyscore and PRISM show broad scale surveillance is here, and we should not only protect our communications, but also the mere existence of our communications networks.

Protecting the existence of your networks begins with the knowledge that you even have secure communication networks. Avoid the urge to talk about them electronically; instead opt to educate other members face to face. The regime doesn't need any help to identify you.

One Time Pads.

A One Time Pad (OTP) is a method of manually encrypting messages, which, if done properly, is widely regarded as able to produce impenetrable encryption. An OTP message has multiple benefits but also just as many downsides. For one, you will trade away efficiency for security. Manually encoding OTPs – the only way it should be done – can be time consuming, and is prone to simple errors of mathematics. Simple errors will cause small problems (such as a wrong letter in the message); larger errors can corrupt an entire message. Shorter messages are better as you will cut down on room for error, and the message can be transmitted in a shorter amount of time.

One Time Pad messages are vulnerable in two ways. Typically, two elements that communicate will each have a booklet of the same keys. If you have ten keys, then you can send or receive ten messages; a hundred keys, a hundred messages. Should either key booklet be discovered, not only is the possibility of communicating with your agent now null, but future messages to him could be compromising. Imagine a scenario where your key booklet is discovered, and the regime is now able to send messages to your agent on your behalf. The first regime message might be to meet at a specific location, where the agent is identified; followed by further instructions to make contact with other agents. With the use of targeted surveillance, the compromise of one booklet could spell the end of an entire resistance organization.

Alternatively, should the message itself be discovered, although the regime analyst will not likely be able to decrypt the message, its appearance is glaring: it's plainly an encoded message. Regime discovery of an encoded message is certain to draw scrutiny, especially in non-permissive environments. If discovered, an OTP message will be confiscated for exploitation, rendering its content moot and irrecoverable. In order to avoid confiscation, you should disguise the OTP message, if at all possible. A list of telephone or social security numbers, or an accounting slip is a plausible disguise for a numeric OTP message. A 10-digit telephone number is just two five-digit OTP groups.

Example OTP
69395 75991 57119 90813 87399 12765 02381

Telephone Numbers
693-957-5991
571-199-0813
873-991-2765 ext. 02381

SSN's
693-95-7599
157-11-9908
138-73-9912
765-02-381?

In addition to keeping the keys physically secure, the one-time in OTP dictates that each key is used only once and then burned, shredded and mixed with water, or otherwise destroyed. Upon receipt and decryption, each message should be destroyed as well.

If regime elements are tracking your resistance cell and discover that you use OTPs to communicate, they will certainly make deliberate attempts to find your pads. You need to have planned an alternate method to communicate that the pads and all captured messages have been compromised.

Be prepared to identify which messages, if any, were compromised, and any sensitive information contained in those messages.

Links to technical information on OTPs is available in the Appendix.

TRADECRAFT.

Steganography.

Steganography is the technique of hiding a message, or ‘payload, inside of an innocuous cover file - these could be images, videos, sound files, or a message. Providing cover for your payload might allow it to pass through a security gateway with limited or no scrutiny. In the event that it does not, you should always encrypt your payload, and do not count on steganography alone.

You must use original content for cover files. If you take a random image off the internet and reuse it, then detecting the difference between the cover file and your payload+cover file is a trivial task. File sizes could be compared, in which case a discrepancy will be identified.

Although email is one channel to send steganographic messages, also consider websites that allow free, anonymous, time-limited image and text hosting. Agree on a schedule and a keyword with your team, and then post steganographic communications via Tor. Also try using steganographic techniques in various blog comments. Identify popular blogs or websites that accept comments via Tor to ensure you maintain your anonymity.

Cryptonyms.

Intelligence agencies around the world utilize cryptonyms, or ‘code words’, to hide sensitive information in communications. Because of the inherent risks associated with communication, a resistance organization should utilize code words and codes to conceal identities, plans, or other details.

For instance, if a communication that you need to trade ammunition for medical supplies is intercepted, then you will give the regime analyst very important data about the condition of your organization. Therefore, you'll want to communicate that message using code words. Ammunition's code word might be 'tulips', and medical supplies might be 'roses'. If a message was intercepted that you wanted to trade tulips for roses then it may not be given a second glance, and would provide your courier some level of cover in case the message is given any scrutiny. Even if the message is intercepted, you will greatly mitigate the damage caused by information discovered by the regime.

One important element in the successful use of codes and code words is ensuring that your code words agree with their cover. A message of trading 'tulips' for 'roses', if carried by an individual with cover as a gardener, shouldn't raise any red flags. A pastor with a written sermon about 'Mark' and 'Matthew' is not suspicious. Offering to purchase 'red' or 'blue' is suspicious; offering to purchase a 'Labrador retriever puppy' is less suspicious.

If your code words, or someone with familiarity with your code words, are compromised, then you should re-code all sensitive information. The longer your code words are in use, the more susceptible to compromise they may become. Altering code words organization-wide is a difficult process, so be deliberate in your plans. Identify how you will securely notify each individual as to which code words have been changed.

Your organization should also make use of code words to name upcoming operations or other developments. OPERATION ENDURING FREEDOM, OPERATION DESERT STORM/DESERT SHIELD, OPERATION MARKET GARDEN, and OPERATION OVERLORD are all well known examples. Alternatively, a short sentence of phrase may be less conspicuous. 'The yard sale' or 'the open house' meet the same requirements. Utilize effective code words or phrases that provide cover and concealment of your actions or intentions.
Along with the code word, another popular form of cryptonym is known as the digraph – two letters that refer to a specific piece of information. For instance, the CIA referred to itself as KU, and referred to different mem-

bers or facets of its organization by other cryptonyms such as KUBARK, KUKNOB, KUMOTHER, and KURIOT, with each word following KU referring to a separate element. Similarly, the United States was known as LN, and the United States Government was known as LNHARP.

It may be the case that you utilize separate code words for different tiers of your organization. For instance, top tier leadership (cell or regional) may utilize the digraph cryptonym when referring to upcoming operations or other plans, and middle or lower tier members use simple code words.

A code name or code can also be a set of numbers, such as a brevity code. When sending messages over unsecured channels (radio transmissions, cell phone texts, unencrypted emails, internet forums), utilize number codes. Many law enforcement use 10-00 (ten double zero) instead of 'officer down', 187 instead of 'homicide', and 211 instead of 'robbery'. In addition to masking sensitive information and obscuring the meaning and intent of communications, using cryptonyms will also conserve space in messages when sending an OTP.

DIGITAL SECURITY.

Anonymous Communication.

VIRTUAL PRIVATE NETWORK. A VPN is a tunnel that encrypts and re-routes your information through a separate server, and assigns you a new internet protocol (IP) address which affords you an added layer of protection.

Anonymity and anonymous communication is a keystone of resistance. Relaying information to others without identifying yourself is critical to disseminating information in non-permissive environments. Videos or photographs of regime brutality or news articles are examples of media or information you might want to distribute anonymously.

Virtual private network.

VPNs can be visualized as a tunnel to a remote endpoint from which your traffic emerges and heads to its final destination; leading that final destination to believe the remote endpoint is the actual origin of the traffic. For example, you present each website you access with your internet protocol (IP) address. From your IP address, the website and anyone with access to the data can see your general location. By using a VPN, you are masking your location by using a separate and representative IP location. For instance, the IP your internet service provider gives you may be based in your hometown – Anytown, USA – but by using a VPN, your new IP address resolves to Dallas, Texas (or where ever the servers are located).

Alone, VPNs offer reasonable protection against non-state entities. Your payment to a VPN service, however, will associate you to the VPN IP address. Do not use a VPN alone to launder your traffic. As of the writing of this manual, there is some question as to how broken VPNs are in the face of NSA snooping. Further revelations may indicate that this is not a technology you want to solely depend on to launder your connection. Blended techniques with Tor (and services similar to Tor) will provide better security. Presently, the only VPN service you should consider is one that you can pay for anonymously, if that is your only COMSEC method. The regime will likely have the ability to identify you by your VPN IP, and retrieve your personal information from the company.

Tor and anonymous browsing.

Tor is a network of volunteer relays, which is free for clients to use to launder their Internet connection. It's a great way to anonymously browse websites that might subject you to regime scrutiny, and is critical during the collection of Open Source Intelligence (OSINT) information due to the regime's ability to otherwise track your online movement.

As a client connects to the network, Tor chooses a 'circuit' of relays, and launders its connection through them. The Tor service then acts as a firewall of sorts, effectively anonymizing your web traffic. Tor is a great service but shouldn't be used by itself. Using the concept of layering, you'll also want to include other techniques to lower your profile.

There has been some speculation as to how anonymous Tor connections are, and quite a few caveats to its use. Tor is open source, so public security issues are usually dealt with in a timely manner. Resistance cells are urged to have someone in their group detailed to keeping abreast of current news on the project's website.

Online chat.

Off the Record (OTR) is an encryption suite that sits on top of any internet chat protocol, and provides authentication, deniability, and strong cryptography. Currently, the protocol only allows one-to-one chat (as opposed to a 'room' with many participants), and it does not provide any sort of anonymity. There are many chat servers that will allow Tor connections, however, TAILS makes this method of conversation extremely easy. The ability to deny collection of a conversation's content can be extremely important, and OTR is one of the only ways to accomplish this online.

Telephonic communication.

Because of their ubiquity and the habits of most users, cell phones are terrible from a security perspective. We must re-think the use of cell phones, and what sensitive information can be collected from them. For the regime analyst, not only is the cell phone is a treasure trove of historical data, but it also might be the single greatest collection tool he has available.

The regime's spying tools encompass all cell networks. The degree to which they can track the physical location of your cell phone depends largely upon how many towers your signal pings off. It's widely regarded that three cell towers will geo-locate your location to within a few feet. Many cell phones, however, give away your geo-coordinates through locational services no matter how many cell towers are in range. The only way to shut off the signal is to remove the battery. The battery should be removed when the cell phone is not in use.

Sometimes cell phones will greatly aid your operations and communications capability, and you might encounter scenarios where not using a cell phone is generally impractical. Although cell phones are collection nightmares for the resistance cell, a cell phone can still be useful if utilized correctly. The use of 'burner phones' is one way to mitigate the risk associated with cell phones.

While the same geo-location principles apply to burner cell phones, these phones aren't associated to any specific individual because these phones don't require contracts. Use pre-paid cell phones that are only used for a limited amount of time and then discarded. These burner phones often use month-to-month calling cards, and by purchasing these phones and calling cards with cash, you will greatly increase your ability to remain anonymous even though the information transmitted and call location is still collected. Also keep in mind that using a burner phone in any proximity to your personal cell phone will co-geo-locate them, in which case you have just burned your personal cell phone, along with all previous communications.

Tools in current use by NSA are able to create and track a virtually infinite web of associations. Any number you dial will be automatically added to this web, and through its exploration, the regime analyst will be able to make direct and indirect associations that greatly increase his awareness of your network and sphere of influence. Not only can time, duration, and connection be analyzed but also locational data.

Because even burner phones' geo-locations are logged, consider the concept of the 'pattern of life' of the phone. Be aware of what locations you use the phone, and how its usage and geo-location could cause problems in the context of other surveillance tools. For instance, using a tracked cell phone in view of surveillance cameras would give away more than just the cell phone's location. Utilizing a burner phone suspected of resistance activity in proximity to a family member's cell phone will likely spur regime intrigue on that individual.

Radio.

There are several off the shelf solutions for secure short range radio communications. Motorola encrypted radios appear to be the gold standard, but are extremely expensive. Newer models use high-grade cryptography that is very attractive, though still vulnerable to direction finding. Trisquare radios are a less expensive alternative that use frequency hopping (not to be confused with encryption) to elude eavesdropping.

Direction finding poses a significant risk to continued transmissions. Direction finding equipment is able to track the point of origin of radio signals, and will allow regime elements to potentially quickly locate the source of transmissions. To decrease your exposure, remember that short transmissions are the best transmissions, and transmissions from fixed locations can be easier to locate. While the availability of complex direction finding equipment is finite, there exists the possibility that the regime is using it in your area in their attempts to find and/or collect on you.

Dead drops.

A final method of anonymous communication safe from electronic collection is the dead drop. Dead drops are a method whereby one individual 'dead drops' a message or package at a specific location, and the intended recipient is told where to find the message or package. Dead drops help prevent the arrest or disruption of an entire resistance network by making associations more difficult to establish. Further, the dead drop allows compartmentalization of information, as you can control what information or materiel is provided, and to whom our messages are given. The ability to send physical messages anonymously is a key utility of the dead drop.

The sender often uses a specific signal – a store window sign, chalk marks, a light in a window – to notify the intended recipient that the dead drop has been made. This method allows communication without arousing suspicion, and mitigates the risk associated with a live meeting of two individuals. In larger networks, couriers can be used to move data from one dead drop location to another, further helping to insulate cell members from each other.

You may dead drop a message on a piece of paper or memory stick, or you may dead drop a weapon or ammunition to an agent, or cash in an envelope to a source. The contents make the location and the security condition surrounding a location critically important. While dead drops keep communication offline, and therefore outside the purview of the digital surveillance state, with the exception of built-up areas where security cameras or overhead surveillance may persist, the dead drop is safe from most surveillance. Ensure that the sender and receiver, however, are not under surveillance before making a dead drop. It's a sure way to compromise all future dead drops at the same or other locations. Additional notes on surveillance are covered in the chapter on Personnel Security.

Meta-data.

Signatures and fingerprints are important to be aware of and to conceal. All digital cameras (to include the worst offenders: cell phones) embed some sort of fingerprint on their images, and for the resistance agent, these fingerprints need to be sanitized as close to the camera as possible. Sanitizing has many techniques of varying complexity - from removing EXIF tags, to remapping the camera lens characteristics. Producers of content may want to change their mode and modus operandi every so often to complicate forensics attempts.

Computer documents created by Microsoft Office and other programs could contain sensitive information in its meta-data. Plaintext documents (.txt, for instance) are best for distribution of typed information since these documents contain no meta-data.

A final note on COMSEC: Your security can only be as good as you make it. Just because your COMSEC doesn't appear to have been breached doesn't mean that it hasn't been breached. Practicing good COMSEC, however, is only one part of the security battle. Information Security is a critical component of your security.

NEXT STEPS

1. Generate a secure OTP (use an analog process such as rolling ten-sided dice - do NOT use six-sided dice) and distribute it through a non-digital channel (courier, direct hand off, dead drop). Practice communicating with your OTPs via pen and paper encryption alone. Destroy the OTP after use, and never reuse an OTP.

2. Start using cryptography for every communication you reasonably can. Even if the information itself isn't sensitive, perfect practice makes perfect.

3. Secure your endpoints. TAILS has been the best choice for this for some time and requires only a burned DVD (or flash drive) and a reboot. It is possible to use the software available with TAILS to get everything you need done securely, and you can always switch back to whatever system you are more comfortable with for your 'cover' activities via another reboot.

4. Start paying attention to your cell phone: where you take it, when it's on, what you use it for. Begin modifying your patterns of life to consciously exclude it. Turn it off for your commute, stop reading sensitive materials with it, and stop using it to write incendiary emails. Begin a new pattern of life that is more resigned about the present state of affairs.

5. Start using Tor to browse sensitive sites. Even if you are on a list, you will begin to lower your profile such that regime analysts need to work harder to keep tabs on you. Eventually, either the amount of work required to keep tracking you will become prohibitive, or enough individuals on lists will drop off that it will send a message in itself.

6. Start practicing with dead drops. Identifying where your dead drops are secure from public interest is something to learn now. Drop OTPs or inexpensive material goods, and see how long a message can sit without being disturbed.

CHAPTER TWO

INFORMATION SECURITY

"An ounce of prevention is worth a pound of cure." Benjamin Franklin

Information Security (INFOSEC) is the program we use to secure our stored information from compromise. Securing your sensitive items, documents, and digital information through robust security measures is absolutely critical because spillage of any information can result in death, capture, and/or destruction of entire organizations. INFOSEC is important not just because we want to protect our sensitive or classified information but because we want to protect all information.

Through electronic intrusion and surreptitious collection, tyrannical regimes gain information from unsecured information systems (computers and storage devices). As a resistance organization, we cannot reasonably suspect that any method of collection or coercion is off the table, which significantly increases our motivation for implementing good INFOSEC measures.

Sensitive information is anything that, if discovered, would pose a considerable risk to operations or personnel. Whether our information is discovered through electronic or physical intrusion makes little difference. Examples of sensitive information include personnel information, intelligence reports, source information, operational details, communications, and plans.

One question we need to ask ourselves is, "How do we achieve our security objectives, and secure our sensitive information both electronically and physically?" Security measures will almost always be the result of a thorough threat analysis (covered in Chapter Four), and the security measures we implement should be commensurate with the collection threat and sensitivity of the information. The threat to an average citizen's grocery store list and the risk associated with its compromise are both low, so he leaves it on the fridge. The collection threat to a resistance organization's sources or safe house information is high, and so is the risk associated with its compromise, so we heighten our security measures over it.

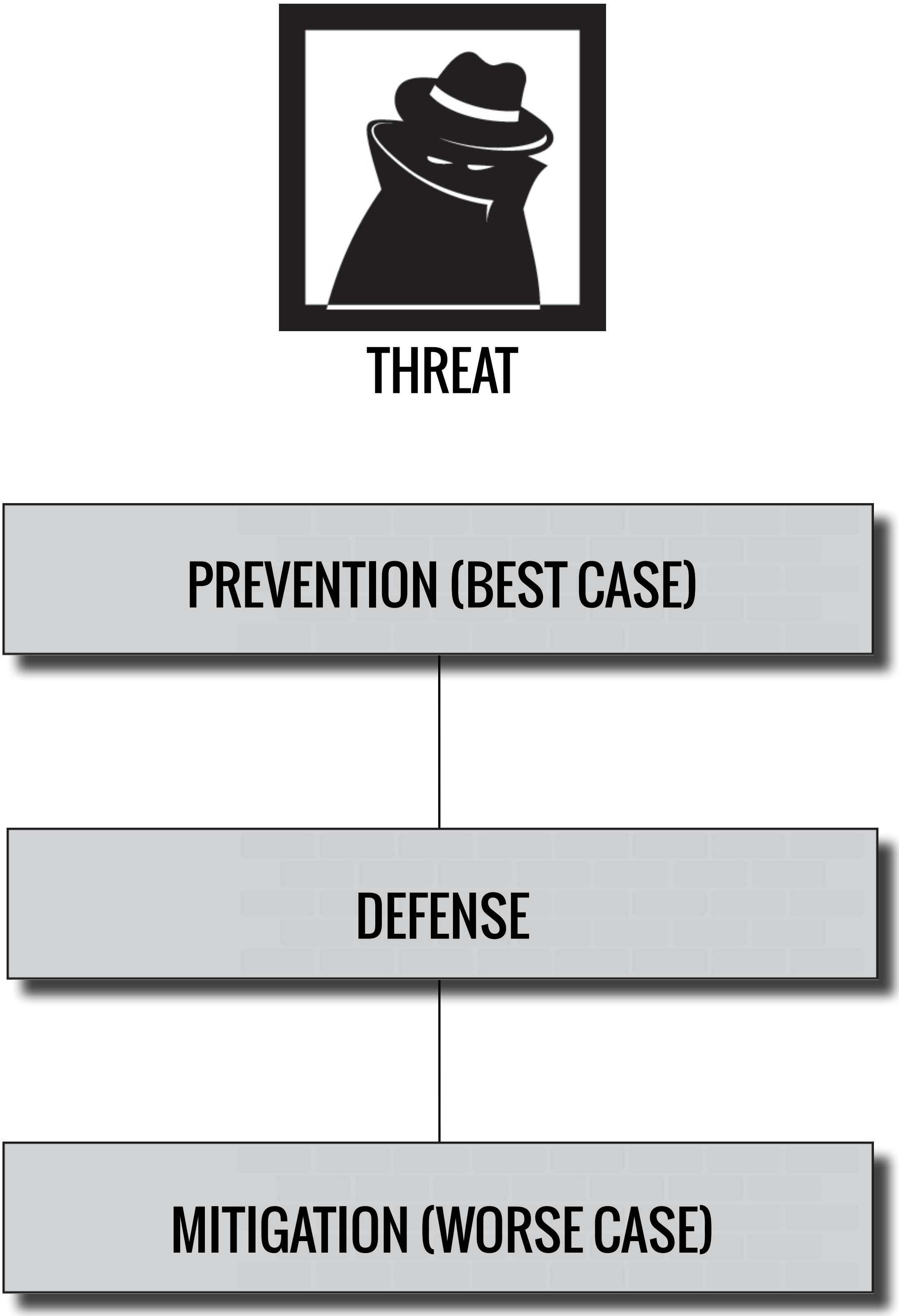
Develop your INFOSEC program in the context of three categories: information accessibility, handling, and storage. Who has access to your information systems, who handles your information (couriers, for instance), and how do you store your information? When answering the how of INFOSEC, we utilize these three categories of security measures.

Prevention.

Prevention of unauthorized access, manipulation, capture, or other forms of compromise is the most solid security measure. When dealing with protecting information, we must play defense first. With some planning, foresight, and knowledge of our vulnerabilities and the collection threat, we can limit the threat posed by our adversaries by implementing preventative measures.

The first general principle of prevention is to secure your platforms. This means getting off Windows and iOS, and getting onto a stable, secure, and open-source operating system like Linux. In light of new information, we know of the regime threat through backdoor access to popular operating systems and the information stored therein. If targeted by regime elements with the capability to gain access to your computer electronically, your follow-on and physical security measures are a moot point.

The preparation of an awareness program tailored to information systems and information handling should be seriously considered. Any member,



THREAT

PREVENTION (BEST CASE)

DEFENSE

MITIGATION (WORSE CASE)

regardless of role or responsibility, who utilizes a computer or handles sensitive information should be familiar with appropriate security measures. Security is only as strong as the weakest link. Do not allow a misunderstanding or lack of training cause a security violation that allows sensitive information to be collected. Make your members aware of the collection threat.

Although it might be cost prohibitive, your organization should utilize a stand-alone computer system that isn't and will never be connected to the internet, and that stays in a safe, secure, and 'off the radar' location. This is where you store mission-essential information systems and your most sensitive information; items that would pose grave risks should they be compromised. You might even consider using a safe to prevent theft or unauthorized access. Additionally, access to and knowledge of this stand-alone computer should be strictly limited. Begin an access control program, and allow access to your workstations only by vetted individuals.

Along with an access control program, realistically designate the importance of information and mark it appropriately. You might use UNCLASSIFIED, CONFIDENTIAL, SECRET, and TOP SECRET, or you might have your own classifications. Either way, delineate what needs to be afforded special protection (organizational, personnel, source, and operational information) from what doesn't, and then disseminate this information through appropriate 'need to know' channels.

Endpoints of communication, e.g. your workstations, need hard disk encryption. Encrypting hard drives can guard against spillage in the event that you are compromised. Beginning users should be using "whole disk" solutions that require a password even to boot, so that no accidental leaks happen between different domains on the drive. More advanced users may prefer to keep their sensitive data within a hidden volume, making sure that their user habits don't leave inadvertent fingerprints unencrypted. Encryption software such as TrueCrypt will allow you to encrypt an entire hard drive, or a portion of it.

To ensure consistent security measures, develop an organization-wide

INFOSEC standard operating procedure (SOP). This SOP will detail how information is protected and stored. Your SOP could be as simple as a list of rules, or as complex as a categorical guide. Make sure to detail what steps should be taken if and when the SOP is violated. Minor violations may not require further action, however, larger violations may require that current operations, plans, locations, and personnel are modified due to compromise of critical information.

Defense.

Should your preventative measures fail, be prepared to defend your sensitive information, both passively and actively. Your entire organization is depending on the security of sensitive information. Should you fail to adequately protect those documents from the regime, your organization will probably be eradicated.

Conducting a realistic physical security site survey and vulnerability assessment is crucial to determining and improving the integrity of an existing building or infrastructure. Some things we want to consider are perimeter entry ways (access roads, drive ways or fences), exterior and interior (secure area) entry ways (to include windows and air vents), exterior walls, electrical systems and availability of electrical power, personnel with current or routine access, and existing security measures. Attempts to break physical security could be as simple as cutting the electricity to your safe house, or as complex as an electronic attack or raid. Identify your vulnerabilities, assess how critical (or relatively trivial) an impact any exploitation would make, and build on existing infrastructure to improve your physical security.

Passive defensive measures include intrusion detection and early warning systems such as motion sensors and alarms, and automated surveillance like security cameras. A strategically-placed motion detector that triggers a light when tripped could give you a thirty second warning to destroy your information systems. If your secure area exists in a home or office building, be sure to include a mechanism whereby an exterior sentry can signal an intrusion. It might be an intercom call, a buzz alert switch, or a light switch. While you may consider these items overkill, even the threat of passive security measures will make surreptitious collection more difficult.

In the event that your secure area is breached, simply shutting down your computer isn't enough. Through what's called a 'cold boot attack', regime information technology (IT) specialists could recover the keys to your encrypted computer, and gain access to the information therein; typically, for up to ten minutes after shutdown. Destroying the RAM modules of your computing hardware is critical to preventing unauthorized access after capture. A thermite cannister is a popular anti-materiel device for those who can legally own them. Once you identify where the RAM modules are located in your computer, a few pistol, rifle, or shotgun rounds may have to suffice.

The other physical defense measure under a worst-case scenario is going to guns. When operating a safe house in a non-permissive environment under a tyrannical government, you must be willing to defend your sensitive information through any means necessary.

Mitigation.

The third category includes the mitigation of consequences as a result of compromise. In addition to your INFOSEC SOP, you should plan for the event that your most sensitive information is compromised. You may be forced to modify or re-arrange all your previous practices, or you may go completely dark and rendezvous at a pre-determined location, but you must develop a plan to alert your teammates that the worst has happened. Even this presents its own security challenges: if your teammates are under surveillance, and you make contact with them, your communication could compromise your own security situation. Only you can make that call based on your own moral and ethical values.

The Twentieth Century is rife with examples of spy, resistance, and insurgent networks being completely obliterated as the result of the compromise of one team member. Retribution or so-called justice has been swift, and we should expect the possibility of retribution with no less speed.

All known and suspected spillages, compromises, intrusions and violations, along with unexplained modifications to hardware or software, malicious infections such as Trojan viruses, the presence of suspicious files, and any other irregularity should be reported as soon as possible to the intelligence officer, security manager, or leadership.

Prepare to conduct a damage assessment in order to mitigate any possible damage: what was leaked and what are the likely effects? Which sites are a security risk, and are there any sites that can still be considered secure? Do you need to recover personnel? Should each team member hit a pre-assigned rendezvous point and await further instructions? Your number one priority should be to stem the hemorrhaging from strategic shock to your organization. Prior proper planning will greatly aid your survivability, and quicken the return to operations, if at all able.

Another way we mitigate damage from compromise it to back up our sensitive information. If successful in destroying other hardware, will you, in the future, need access to the information contained on that machine? Although we may be able to return to operations as a result of a copy of our sensitive information, backing up that information poses another security risk: now you have two storage devices with sensitive information instead of one. These are all factors that each organization should consider in order to develop its mitigation strategies.

CHAPTER THREE

PERSONNEL SECURITY

Identity management is an important piece of Personnel Security (PERSEC) and identity information denial. Whether you operate openly using your real name (not recommended), operate under a pseudonym or code name, or operate anonymously, your identity should be protected at all costs. 'Identity Dominance' isn't just a catchphrase of the surveillance state; it's a way of life for Identity Intelligence teams. Once your true identity is discovered, it cannot be un-discovered. Once your name and face have been associated with resistance activity, and distributed to the public, there is little you will be able to do openly. In a resistance movement, there is more at risk, however, than just identities, and providing security for your personnel is a critical piece of keeping you in the fight.

Personnel security controls.

Personnel security controls are how we protect personal information in the course of official duties. One option is to mask identities. Every member of your team should utilize a code name in place of his or her real name, and these code names can be as open or secret as you want to make them.

We can control what personal information is distributed through granting access to information only to certain individuals based on their duties, and denying access to all others. We deny identity information to the regime through compartmentalization. 'Separation of duties' is a form of compartmentalization. By separating duties and creating different levels of information availability, we can protect our identities from those who don't have a need to know. Although some identities will be known by way of prior relationships or acquaintances, a small segment of your organization will know how the code names correspond to individual identities. Compartmentalization of identity information will greatly aid the security of your organization should a compromise occur at any level.

Anonymous or pseudonymous authentication is a process where individuals use a challenge and password to authenticate each other, without knowing their counterpart's identity. For instance, an asset may receive a challenge ("Nice weather we're having."), and the handler responds with the correct password ("Yes, and the stars are bright."). Authentication comes from a specific, prescribed combination of words or phrases without requiring identity information to be exchanged.

Code names.

Code names, pseudonyms or call signs are a mainstay of resistance organizations and other sensitive operations. For one, they effectively mask our identities, and provide us cover, and for two, they can easily be changed as the mission requires, or in the event of compromise.

Just like other security measures, code names are only as effective as we make them. While it might be easy to assign the code name "Red" to the guy with red hair, assigning a code name that's also a physical description defeats its purpose. Whichever code name you assign or adopt (Reaper, Mustang, Nighthawk, for example), ensure that it provides adequate cover.

Pseudonyms are fake names or personas that provide us operational cover and that we use in place of our real names. Using a pseudonym like Brian Watkins or Steven McCandless is perfectly acceptable for one-time communications where you want to keep your real name a secret. For continued contact with acquaintances (recruiting a intelligence source, for instance), Brian Watkins may be an adopted persona; a salesman from California, or a plow boy from Tennessee. Whichever pseudonym or persona you adopt, ensure that you have the knowledge or expertise to prove your claim.

There's significant merit for mission-based code names, or call signs. Militaries all over the world utilize call signs for their effectiveness, especially over radio. In addition to using names, some call signs use numbers to refer different positions. For instance, Reaper One calls over to Reaper Six Romeo; where Reaper One is first platoon, and Reaper Six Romeo is the commander's radioman. Reaper is the unit call sign, and Reaper Six (or Six Actual) is designated as the command element. Your call signs should be tailored to the operation, and easy to communicate and understand. Best of all, call signs can be changed for the next mission to avoid forming a pattern.

Biometric threat.

'Biometrics' is simply a measurement of identity. Bio, meaning life – namely human – and metric, meaning a measurement: a measurement of human identity, if you will.

Biometrics most commonly includes identifying characteristics like fingerprints, iris or retinal patterns, faces, and DNA. Those things are unique to you; no one has your fingerprints, iris or retinal patterns, or DNA. The concept of 'battlefield biometrics' exploded in Iraq and Afghanistan as Coalition Forces began using simple forensic techniques to discover the enemy's identity.

The biometric threat to resistance organizations – rather, to every citizen – is growing in popularity and capability. Biometric collection and other identity management platforms strip away anonymity from an anonymous individual by associating names to biometric 'modalities': faces, fingerprints, irises, and DNA. The collection and matching capabilities of biometric modalities present an alarming threat that we can't totally mitigate.

Virtually any time your face appears on a security camera, its image can be collected and stored in a database. More and more, facial recognition systems are being implemented, and in the near future we will see near-real time collection and matching across the country. As more law enforcement agencies justify their use, facial recognition systems will receive more investment money and this technology will only grow faster and more accurate. Any photo identification cards (such as a driver's license) already associates your face to your name. The Federal Bureau of Investigation has agreements with up to 26 states that allow them to query Department of Motor Vehicles driver's license photos against the federal facial recognition database. As of now, facial recognition databases can query one face against the entire database (1:n), or a facial recognition analyst/examiner can compare one face to another (1:1). Technologically, and if a comparison can be made, facial recognition systems are probably where automated fingerprint matching was ten to twenty years ago.

Fingerprints have been collected as forensic evidence for over a hundred years. 'Latent' fingerprints – that is, impressions that you leave behind after touching an item – can be collected, photographed, and ingested into a fingerprint collection database. Integrated Automated Fingerprint Identification System (IAFIS) is a routinely-used (24 hours a day, 365 days a year), national-level fingerprint identification system run by the Federal Bureau of Investigation in Clarksburg, West Virginia, although agencies from all across the country and around the world input fingerprints collected from crime scenes and other fingerprint enrollment systems. Through matching algorithms, latent fingerprints are compared against other latent prints (potentially unknown identities) and 10-print cards (or rolled fingerprint cards containing all ten fingerprints of a known individual). The matching system pumps out a number of candidates, and then latent print examiners (LPE) get to work comparing each print to another. Once a match is found, it must be confirmed by another LPE. As you can imagine, this is a very time-consuming process (1:1), and the only way to increase the matching speed is to increase the number of LPEs identifying matches. Further, matches fall into two categories: unknown biometric identities (latent to latent, also referred to as UBIs) and identities (latent to known, or IDENTs). If two latent fingerprints from two separate cases are matched, then we've identified an association between two crime scenes, even though we don't know to whom those prints belong. We could leverage witnesses or known individuals linked to the same crime scene to find out. Be mindful of what you touch; documents, weapons, ammunition, computers, door handles, tables - literally just about anything. If it's considered part of a crime scene and your fingerprints are there, you might wind up as a suspect. This goes doubly for spent brass.

Unlike faces and fingerprints, identification of irises is about 98% accurate and requires no confirmation (other than being matched by the algorithm). The upside here is that it's more difficult to collect iris images, as it requires a deliberate collection process with a purpose-built collection platform. Irises only identify the living, as the iris patterns begin to degrade upon death. When the state rolls out iris capture platforms, the only possible use is to identify living individuals.

Finally, our last modality is Deoxyribonucleic acid (DNA). The DNA matching process is the most laborious of all. It requires that DNA be collected, free from contamination from a collector, shipped off to a DNA processing facility, like Armed Forces DNA Identification Laboratory (AFDIL), processed, encoded, and finally matched based on its profile. Just like irises, there's no room for error on DNA matching. What's worse is that you drop your DNA through skin cells and hair follicles all day, every day. Since the average individual loses up to 100 hairs a day, you're likely leaving around a pretty thick trail. Also keep in mind that the matching abilities of DNA are extensive; DNA matching can identify others as being your blood relatives, either on your mother's or father's side.

Overseas, biometric collection platforms were fielded across Afghanistan and Iraq, and US and Coalition soldiers began collecting images of faces, fingerprints, and irises under the mantra of 10-2-1: 10 fingerprints, two irises, and one face. As the enrollment databases grew and more and more latent fingerprints were collected from attacks and other "crime scenes", biometric watchlists were created and loaded onto biometric collection platforms, such as the Biometric Automated Toolset (BAT), Handheld Interagency Identification Detection Equipment (HIIDE), Cogent Fusion, and a handful of other devices. Once enrolled, individuals' biometric information was queried against the loaded watchlist through the matching algorithm, and returned with an identification, if able. Some of these identifications were false positives – that is, an error in the algorithm made an incorrect match – and other times the devices were capable of false negatives – that is, failing to match an enrolled print against the watchlisted print. Most of the time, however, these devices were very good at what they did, and gave soldiers in the field a leg up on ending anonymity in the insurgency.

Biometric collection is already occurring in the US. It's now lawful for DNA to be collected, in addition to rolled fingerprints, after an arrest. This allows law enforcement agencies to identify and capture legitimate criminals, but it also poses a direct threat to any resistance movement. In a situation where resistance to unconstitutional action or martial law occurs, although a resistance member may not be arrested, he may have his biometric data captured by a biometric collection platform under a fake name. That fake name is now tied to real biometrics. If enrolled again, and a different name is given, then he's going to present a red flag to the enrollment team.

One concept pioneered only a few years ago in Afghanistan is that of the tactical biometric collection operation. Through analysis of patterns of life and the timing and location of certain events, a regime analyst may surmise that questionable individuals may be located within a certain geographic area of a few square miles. Although it's a considerable feat, enrolling every man, woman, and child inside that operations box won't likely be impossible to achieve. If the analyst's assumption is correct and the juice is worth the squeeze, the collection operation will cast a biometric net in the area, and identify those suspected or watchlisted individuals. If and when offensive biometrics takes off in this country, and the author believes that it's only a matter of time, tactical biometric collection operations will be here to stay with a frequency and aggression commensurate with the viscosity of resistance in any given area.

Be aware of so-called 'battlefield biometrics', ensure your teammates understand the threat, and how to counter it. Remember that biometrics is a supremely useful tool that politicians and law enforcement agencies have grown both to understand and love, and its value in recent years has skyrocketed. In any situation where resistance to tyranny becomes duty, your task is to identify known collection points, and either avoid them or counter them.

The best way to counter the collection of your biometrics is to simply not become a victim. Once your biometric data has been collected under an emergency, it will likely be there forever. If history is any indicator, there won't be any 24-hour or seven day deletion requirements. Failing that, if regime forces attempt to illegally collect your very personal biometric data, then you should have already made some plans.

Because facial recognition systems use sophisticated algorithms based on position and distance of recognizable facial features, our only recourse is to make them harder to identify by obscuring or hiding those features. Wearing sunglasses, or using makeup or shading is a great option. The best alternative, of course, is to map out these surveillance cameras and avoid them at all costs.
For fingerprint enrollment into digital devices, dirt in between the ridges of your fingerprints could cause a bad capture initially. You should, however, expect for enrollment teams to wash your fingers before collection, as it will likely be enrollment SOP. Some have attempted to burn off or mutilate the ridges of their fingerprints but that will likely draw more attention and scrutiny. Although being slightly uncooperative could raise suspicion, your goal, should you choose to be enrolled, is to cause as incomplete an enrollment as possible. Because we know that the index fingers and thumbs are the most commonly identified fingers, consider lifting up an edge of each of these fingers for a partial print enrollment. If you get a bad capture on the finger, they will likely just enroll you again. Your last recourse, short of avoiding or evading collection, is to either break the collection platforms, or break the collectors. Those are your only options.

Your irises will likely be collected using the same platforms as your fingerprints, so the rules generally stay the same. Wearing contacts that obscure or replace your iris patterns is a viable option, if undetected.

You deposit your DNA virtually everywhere. For the regime exploitation team, identifying you is a matter of collecting your DNA. Consider what you're likely to touch throughout the day, and remember that you might deposit skin cells, which contain your DNA. Your DNA is likely harvestable from your computer, weapons and weapons accessories, ammunition, keys chains, and door handles, among other things that you likely touch every day. The only way to beat DNA identification is to avoid leaving it behind.

Social media.

If you don't already know it, the internet is forever. Once information has been posted, it's been logged, archived and catalogued. In many cases, there's no un-posting it.

Facebook should be considered the scourge of resistance movements. Really, just about any social media should be considered the scourge of resistance movements. It's speculated, probably accurately, that regime spy agencies have cart blanche access to social media sites. Therefore, what you say and to whom you say it are both critical security issues.

If posted, photos of you and your family, names of family members, where you work, what you do with your free time, who else you know and where you've been, among other answers to countless question, become available to the regime analyst. Simply put, social media sites are a regime intelligence treasure trove. Don't offer them any freebies.

If you do choose to continue using social media sites to stay in touch with family, keep in mind appropriate security measures, especially communicating pseudonymously. There's no reason for the regime analyst to view one page and, within several minutes, be able to flesh out an entire resistance cell or network.

Risk management.

Perform a risk assessment on yourself and the members of your organization. Are there any loose cannons with penchants for adventurism, proverbial loose lips always sinking ships, or oddly suspicious characters? If so, it's okay to identify these people before they identify themselves.

Consider their circumstances and if their skills are worth the added risk of keeping them around. If you must keep them around, consider how they fit into your personnel security controls; that is, how much they will know (or learn), and when they'll know it.

Personal security.

As with other layers of security, the measures you take should be commensurate with threat and risk levels. You might treat a trip to the grocery store differently than you treat traveling to a source meet or to dead drop contraband to an agent. Being aware in each situation should be standard practice but intelligence collection of potential threats, a route study, and accompanying security may not be necessary in every situation. It might be easy to view the size and scope of the surveillance state, and surmise that you are under physical surveillance. The fact of the matter is that the average American isn't being targeted by surveillance, and neither is the average resistance fighter. There aren't enough resources to physically target everyone with active surveillance. If you take adequate security measures (COMSEC, OPSEC) then you will likely be just another nameless face in the crowd.

It's impossible to be on 'red-alert' for 24-hours a day, and attempting it is an exercise in futility. Whether or not there's a transparent physical threat or threat of collection, implementing physical security measures and keeping a security-oriented mindset is a habit. We sharpen that habit through practice and repetition, and being sharp can prevent personal attacks and surveillance, whether from a street criminal or a regime criminal. When it's time to flip the switch, or when the switch is flipped on you, is not the time for practice. Be aware, however, not to slip into the 'persecution complex', where you feel that everyone is always out to get you. There's a difference in being ruthlessly paranoid and being aware.

Developing a strong situational awareness is paramount, and a chief task for the operational resistance cell member. Being alert is the single skill that's prevented more ambushes than any other action. Being able to observe and understand your surroundings and identify irregularities, including signs of surveillance, is skill you'll have to constantly develop. The use of overhead assets like drones as a surveillance method can't be ruled out, and presents its own set of critical security issues. You simply won't know, no matter how alert you are, that you're being tailed by a drone. Still, recognizing that you're potentially under surveillance will greatly increase your security situation.

There are three types of surveillance that concern a resistance organization: fixed, mobile, and surreptitious. An example of stationary surveillance is a 'stake out' in a neighboring house or office space, or a parking lot security camera. Fixed surveillance is used when you are expected to be in a limited area, such as your home or work. An example of mobile surveillance is a tail, an individual who's been tasked with following you by foot or vehicle (or by air). The regime may use mobile surveillance to follow you to meet a source or to make a dead drop. Finally, surreptitious surveillance includes the use of planted bugs or eavesdropping devices, or installed computer software such as a Trojan virus or keystroke logger.

In the event that you are put under targeted, mobile surveillance (as opposed to passive surveillance, such as a security camera), you might be able to detect your surveillant. You can use the acronym TEDD (Time, Environment, Distance, Demeanor) to help spot a surveillant, but keep in mind that professional surveillants are difficult to spot. If you see an individual more than once over Time, in separate Environments, at different Distances, and with a discernible or unnatural Demeanor, then he or she might be conducting surveillance. Ask yourself, does that individual have any particular reason for repeatedly being in proximity? The use of surveillance detection routes, such as walking past your destination and then doubling back or walking in a large circular pattern can also allow you to identify if an individual is in pursuit.

The private security industry offers dozens of different gadgets that allows you to locate surreptitious surveillance devices. These collection devices, often placed in walls or hidden in inconspicuous locations, emit electromagnetic signatures and/or radio signals able to be identified and pinpointed. You might also consider electromagnetic countermeasures, such as scramblers or jammers. Scramblers will cause voice transmissions to be indiscernible without being unscrambled, and jammers will overpower certain radio frequencies used by cell phones or other transmitters. Keep any areas associated with your resistance activities clean and tidy. The more objects in a room, the more areas where a surveillance device might be surreptitiously emplaced.

When traveling, be as inconspicuous as possible so as to not draw attention to yourself, and travel in or with groups if possible. Personal attacks (though not all crimes) are less frequent in areas with a great number of potential witnesses. Traveling in pairs allows each individual to evade surveillance by blending into the environment, or splitting directions. Traveling in pairs also presents a counter-surveillance opportunity where one individual follows a lead, and is then able to spot other potential followers.

If traveling by vehicle, keep it clean and be suspicious of any tracking devices, especially placed under the carriage of your vehicle. It's legal for law enforcement agencies to come onto your driveway, parking lot, or street in order to place a tracking device since you have no reasonable expectation of privacy in these places. If at all possible, use a garage where you can control access; however, if you must park outside, leave your vehicle in a well-lit area. Always lock your doors.

Avoid setting patterns. Patterns make us predictable, and predictability makes us vulnerable. Some patterns are unavoidable – we go to and come home from work every day, but we can vary the routes we travel.

In addition to practicing counter-surveillance techniques, think about identifying what information your surveillant is attempting to collect. Pre-operational surveillance will establish your vulnerabilities, especially patterns, in order to exploit them; or identify your associations (individuals, locations, activities). It can be assumed that he will collect anything he can, so it becomes your job to either deny his ability to collect, or deny him information to collect.

Be secretive about your travel arrangements, and don't communicate them to anyone who doesn't need to know. When researching and developing travel plans, use an anonymous internet browser like Tor. The regime analysts, when perusing your internet search history, may identify that you calculated and mapped the distance to your destination through Google Maps or another service. Ensure that someone close has your travel routes, destination information to include who you're meeting with and how to contact that individual, your estimated times of arrival coming and going, and a way to contact you, at a minimum. That individual should also know what to do in the event that you don't return or something goes wrong.

If handling sensitive information, maintain positive control over it at all times. It's probably best to carry them inside your clothing. If storing sensitive documents or items, then ensure there's nothing missing or out of place. Although surreptitious collection teams will take a photograph of how furniture and other items are situated before they bug a room, even professionals make mistakes.

Finally, keep in mind that your cell phone is more than just a cell phone. Not only can it track your movements but it can also be turned into a microphone. Have all conversations outside of earshot of your cell phone, and remember that the only way to disable a cell phone is to remove its battery.

CHAPTER FOUR
OPERATIONS SECURITY

Poor Operations Security (OPSEC) will lead to mission failure. OPSEC is about denying information to the adversary, and our focus goes into controlling what information goes out. Ensure that the members of your organization understand the regime collection threat, and are educated on the threat spectrum (OSINT, HUMINT, SIGINT, etc.). Poor education or misunderstanding (or underestimation) of the collection threat may be the greatest weakness of your OPSEC plan.

While it's everyone's responsibility to observe appropriate OPSEC measures, the determination of what measures should be taken and the authority to order them comes from leadership and are based on the threat, perceived or real. It's of little concern for a grocery store to implement strict OPSEC measures because there's no high-level threat to justify those measures. A bank, on the other hand, implements strict OPSEC measures because there is both an historical and capable threat. Those OPSEC measures aren't generated by each local branch, but rather by the top of the organization.

Compromise.

OPSEC measures are a safeguard against compromise. The regime analyst will have at his disposal surveillance tools in order to exploit your organizations weaknesses, and compromise the members of your team. Compromise may mean the discovery of your cell's identities, locations, or plans. NSA spying programs have been compromised through unauthorized leakage of sensitive and classified information. American citizens and the rest of the world are now more aware of NSA capabilities, and should take proper OPSEC measures to protect their privacy. Compromise may also mean leverage. A political campaign can become compromised through the discovery that a politician is having an affair. In this case, an opposing politician could put that information to good use, and exploit that identified weakness. Your organization may be compromised as well, in which case compromise would most likely manifest itself as deliberate attempts to have an identified cell member provide details about the rest of the cell. Through the threat of lawfare or other coercion, the regime may learn enough to dismantle your entire cell, resulting in everyone's death or arrest.

Compartmentalization, as mentioned in other chapters, means that very few people, if any, know everything. We are separating knowledge in order to protect it. Beyond that, cell members should only know what they need to know. Knowledge should be sufficiently compartmentalized so that the arrest of one cell member cannot result in everyone's arrest. Further, you may not know that your cell has been compromised until it's too late. Compartmentalize your sensitive information because it's the key to your operational vault.

Critical information.

Adversaries who have the means to collect your sensitive information will attempt to collect it, and they pose a very capable and credible collection threat. Our first step in controlling the flow of information is to identify the most critical information, and compile it into a Critical Information List (CIL).

CRITICAL INFORMATION LIST.

- Identities are not just limited to the names and identities of our leadership and members, but also include facilitators, supporters, and the relation of identities to code names and call signs. ***Who is in your prepper or security/defense group? Who provides support?***

- Locations should include homes and business of members, as well

as safe houses. ***Where do you and your teammates live? Where do you plan to meet up? Where do you store your supplies?***

- Communications include how your organization communicates, on what frequencies and at what times you communicate, what hardware you utilize, email services and addresses, and what communications security measures you implement. ***How do you communicate? How do you plan to communicate post-SHTF?***

- Operations encompass your previous operations (unless you specifically want to publicize them for psychological effects), current operations, future operations, and planning (including planning criteria). SOP includes the inner workings of our organization, and what our standard responses are to events and developments. ***How do you travel? What routes do you take? In what activities are you or will you be involved? What operational materiel do you possess or is required?***

- Tactics, techniques, and procedures (TTP) are what we do and how we do it at the tactical level. ***How do you do the things you do? How do you operate? What's your SOP?***

- Vulnerabilities are our particular susceptibilities. They are our weakest links, our thinnest defenses, and information we don't yet know. ***Where are your weakest links? How are they exploited?***

- Limitations include anything we as an organization are not capable of doing, whether it's tactical, operational, or informational. ***What can't you do? What self-imposed or external limitations have been or will be placed on you or your group?***

Essential Elements of Friendly Information (EEFI) is a list of our critical information posed as questions. We disseminate our EEFI to ensure that each cell member understands what information will likely be a target for collection. Our EEFI is how we turn specific critical, compartmentalized information into questions that everyone can know.

For example, the information about the specific leadership of the organization becomes, “Who are the leadership of the team?” Our specific TTPs become, “What are the organization’s TTPs?” Our EEFI is how we publicize the sensitive information to the entire organization in the context of, “What does our adversary want to know about us?” Included in your SOP should be how the members of your organization go about reporting attempts to collection information referenced on your EEFI.

EEFI List.

Who is in your prepper or security/defense group?

Who provides support?

Where do you and your teammates live?

Where do you plan to meet up?

Where do you store your supplies?

How do you communicate?

How do you plan to communicate post-SHTF?

How do you travel?

What routes do you take? I

In what activities are you or will you be involved?

What operational materiel do you possess or is required?

How do you do the things you do?

How do you operate?

What's your SOP?

Where are your weakest links?

How are they exploited?

What can't you do?

What self-imposed or external limitations have been or will be placed on you or your group?

Indicators.

The regime analyst looks for indicators of your actions when proper OPSEC hides the actions themselves. Observing how we telegraph indicators of our words and actions is of immediate importance.

Indicators are pieces of peripheral information that we emit in the course of our movements, plans, and actions; they're often our invisible vulnerabilities. For example, filling up your vehicle with fuel indicates that you traveled by vehicle in the past, and may indicate that you have additional travel plans in the future. Making a large purchase at the gun store indicates that you are acquiring weapons, ammunition, or weapons-related products, even if the exact products are unknown. Repeated electronic communication with the same group of individuals indicates a close association and familiarity with them.

Identified patterns of indicators present an even more formidable challenge. Developed habits, illustrated to the regime analyst as patterns, are significant vulnerabilities, and must be identified and overcome. To the regime analyst, two of the same events may be unrelated, but three of the same events are a trend. A trend is a pattern just waiting to be exploited.

Identifying these indicators and their patterns should become a priority for your organization. We can use SPACE analysis to become more aware of what our indicators provide to the regime analyst. (SPACE is an acronym for Signature, Profile, Association, Contrast, and Exposure.) SPACE is a cumulative analytical checklist; each topic on its own isn't as powerful as when they're all taken into consideration.

Signatures are identifiable, unique, and stable to an individual or group of individuals. A signature is an encrypted or signed email, or a message from a specific phone or email address, or a semantic tell (the way you speak or write, or a reference or colloquialism in communication). These are pieces of a puzzle that can be collected and analyzed to form a better understanding of individual SOP or TTPs. A signature is something standardized (or roughly standardized) in the way you operate that may identify you as being separate from someone else, much like a signature recipe is to a chef. Serial killers have signatures. Gangs and gang members have signatures. You will never mistake the sound of a monster truck for that of a Toyota Prius, or a dog's bark for a cat's meow. Observed over time, the way you communicate likely presents a signature. These indicators may not always be deliberate, but they're calling cards that help the regime analyst identify a specific, though perhaps anonymous, individual.

Signatures may develop a pattern of indicators called a **profile**. When presented with two separate but anonymous individuals, the regime analyst's first step towards identification is to develop a profile. For instance, in Afghanistan a convoy of jingle trucks led and followed by a pair gun trucks fits the profile of a supply convoy. No one would mistake this profile for that of a US security patrol or raid. In each case, the jingle truck differentiates itself from others by its signature; the same as a gun truck would. You'd never mistake a jingle truck for a gun truck, but added together, we get the supply convoy profile. Another example would be a customer wearing a Ford baseball cap and a John Deere t-shirt in a gas station purchasing $50 of diesel fuel. If forced to guess, would you conclude that he drives a 3/4-ton Ford pickup or a Toyota Prius? If you stopped at a red light behind a camouflage-painted Ford Ranger with two Browning deer stickers and a Size Matters deer antler decal, would you expect the driver to be wearing an Obama '16 t-shirt and a drinking a cup of Starbucks blended no-fat mango mocha latte frappachino with extra whipped cream? In each of these examples, a collection of signatures fit a specific profile.

Associations help adversaries to interpret actions. One step the regime analyst takes to dismantle a resistance organization is to identify indicators and patterns in order to predict a future event. The regime analyst asks himself, is one event associated to another and, if so, what does that indicate about the two events? These events could be phone calls, emails, travel patterns (such as to and from dead drop locations) – all indicators of communication – associated to specific events like a source meet, surveillance route, or direct action mission. In any specific case, he might identify a pattern of control-to-agent communication before an event, and therefore associate the two. In Iraq, perhaps it's the case that when one specific phone number calls another specific phone number, there's a sectarian bombing against the civilian populace the next day, but only when those two specific numbers communicate. That communication is an indicator, and associations between the two are then postulated and confirmed in a future event. The next time those two phones light up, maybe security is heightened, fixed targets are hardened, or the possible target is removed altogether.

Any marked difference in expected communications, actions, battle rhythms, or operational tempos from a profile is called a **contrast**. If Phone A usually calls and communicates with other phones, but only sends texts to Phone B in particular, that's a contrast. It's something outside the normal range of operations. That could be an indicator of a specific future event. If every day for a month you make five phone calls, but one day you make 15, then the regime analyst will observe a contrast in what he's expecting from you. That may indicate nothing significant by itself – maybe your kids are sick and you're calling the babysitter every half hour for an update – but when considered in SPACE, this could alert him to something significant. If your weekly grocery store purchases are generally in the range of $100-200, but one week you spend $600, then he sees a contrast. He asks himself, what does this signal?

Exposure consists of three factors: duration, repetition, and timing, and they each affect importance and meaning. Phone calls placed at random iterations, each lasting for two hours, are an example of duration exposure. The same is said for phone calls twice a day that last for ten seconds.

A text message sent out every night at 1900 is both repetition and timing exposure. Identification of exposure can help the regime analyst form a pattern of life. From there, when combined with other SPACE factors, the regime analyst fleshes out a lot about your organization, even if its members remain anonymous. These things give him a much better idea of where each members fits into the organization.

Enemy collection.

On the other side of the coin, our adversaries also indicate their movements, plans, and actions. It's our job as the resistance element to identify indicators of enemy collection. Even though most collection is passive, due to the vast capabilities of the surveillance state infrastructure to absorb electronic information, we must still consider when the regime analyst has discovered our sensitive information, and what he's doing with it. Identifying how that sensitive information is our first step.

When and if your sensitive information appears to be compromised, resistance organization leadership should immediately identify what information, if any, has been leaked. The mere appearance of leaked information is the most glaring example of compromise. Although the regime analyst considers two events to be unrelated, and three a trend; the resistance organization should consider one event, such as an arrest, as unrelated, and two events a trend. It's then incumbent on resistance leadership to avoid further damage to the organization.

Threat analysis.

Threat analysis is the method we use to understand threats, their capabilities, and their intent. We put each threat under the microscope in order to understand how they operate, to what extent they pose a threat, and what we as an organization can expect from them.

Assess what the adversary already knows about us. We can't protect what's already out there. If it's been communicated openly and electronically, then we have to assume the worst: that information now resides in a vast network of databases just waiting to be plucked at a time when we can least afford it. Make a determination as to the potential consequences of any one piece of information being known. We may want to re-visit planning, change how we're currently operating or will operate, or do nothing and just hope for the best. If you opt for the latter, remember that there were no do-overs for the 170 million people last century who died at the hands of their own governments.

Identify the most likely method and target of collection. We can make a key assumption that the regime analyst doesn't know everything. Therefore, he will be attempting to collection what he wants to know, based off his own intelligence requirements. In analyzing the threat, identifying what he likely wants to know will help us in ensuring that we protect that information. *What does the threat want to know about us? What pieces of information are they most likely to target, and where are they most likely to target it? What's the greatest collection threat, and by what method are they likely to collect?*

- Regime. Everything and anything by method of Human Intelligence (HUMINT – includes surveillance and source operations), Open Source Intelligence (OSINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Technical Intelligence (TECHINT), and Counterintelligence (CI). The regime will have at their disposal any conceived means of collection and each will be used with extreme prejudice.

- Domestic. Gangs and other hostile groups, mostly concerned with targets of opportunity and targets of strategic nature, will pursue their goals including turf dominance and influence. The domestic threat will collect whatever is directly available through HUMINT or OSINT.

- Criminal. Hostile individuals, mainly concerned with targets of opportunity, will not necessarily operate towards any goals other than their own subsistence. The criminal threat will collect whatever is directly available through HUMINT or OSINT as it pertains to a specific target.

- Hackers. The internet is a digital playground for both foreign and

non-state mischievous and nefarious actors. Hackers will likely target public figures and civil servants through SIGINT.

- Insiders. Insiders will overwhelmingly utilize HUMINT but may be aided by external actors through SIGINT. This underscores the need to compartmentalize sensitive information.

Identify indicators of enemy collection. What are the signs that our sensitive information is escaping, or not being kept secret? Are our safe houses getting hit? Are our sources getting worked over? Are we experiencing mission failure? Is any one part of our compartmentalized information standing out? If so, then we have to be prepared to make the determination to radically re-arrange our organization, work to identify our source(s) of exposure, or – worst case scenario reserved for organizational compromise –abandon ship and go dark to prevent further damage to our network. That's a contingency plan that you need to make with your team.

Assess the education and training of our team for the collection threat. An EEFI only goes so far, and collection attempts may not be direct. You may not even know that your critical information is being collected, or a member may be coerced into providing sensitive information. Sit down with your team and discuss the collection threat, ensuring that each member understands that actions and words give away resistance organizations to the regime. Identify and correct deficiencies in OPSEC now.

Regime collection can also be our sandbox. Using the knowledge of the most likely method and target of the regime collection threat, identify how you can use that information to your organization's advantage. For instance, we know that regime spy agencies collect information transmitted electronically. If we know that our information is being collected, what information could your organization deliberately leak in the future in order to waste the regime's time and resources?

Vulnerability analysis.

In the analysis of vulnerabilities, we need to identify what our teammates know, what potential consequences exist if any individual is compromised, and any gaps in our security measures. Tyrannical regimes and other lawless elements are notorious for brutal and often effective collection methods to generate actionable intelligence. Understand that they want actionable intelligence – information that will drive operations right now. For most individuals, intelligence value is diminished over time. What was actionable an hour ago, a day ago, a week ago, or a month ago is now relatively useless except in forming an historical baseline. So what do your people know and how will their compromise negatively affect your organization?

Where are the weak points of your organization? Are you particularly susceptible to the counterintelligence threat, to surveillance, or to infiltration? Are you members properly vetted? The weak point of your organization could be a lack of training, poor operational planning, poor security, poor tradecraft, a poor understanding of the operational environment, the inability to react to an operational environment in flux, or a combination of these things.

Risk assessment.

Risk assessment is where we make our final determination as to what OPSEC measures we implement. What are the risks to the mission if a specific OPSEC measure isn't followed? If a grocery store doesn't encrypt information about when they're getting a shipment of citrus fruits in, there's not going to be any risk of mission failure. They don't need to consider it sensitive information, and their OPSEC measures for that information are going to be very basic; maybe even none outside of compartmentalization (the deli and pharmacy don't need to know). If a small restaurant doesn't protect information regarding the time and route of the closing manager as he goes to the bank to deposit cash, then they run the risk of losing a presumably sizable sum. Losing one night's worth of cash won't put the restaurant's operation in jeopardy, so the closing manager won't need to utilize an armored car. We just performed some risk assessment. You can conduct risk assessment on specific activities or specific teammates. Smart leaders will assess the risk for nearly everything (time and resources permitting).

OPSEC Violations.

Finally we get to OPSEC violations. No one wants to self-report. No one wants to admit that they screwed up and released sensitive or classified information. That's a major reason why most OPSEC violations go unreported. The other major reason is that individuals don't always immediately recognize an OPSEC violation when it happens. But OPSEC violations will bring ruin to your organization, and it's for that reason that you need a reporting mechanism. It could be as simple as a designated OPSEC officer who handles all things OPSEC, or as complex as an anonymous reporting system. Either way, OPSEC violations require immediate action to rectify your current or future operations.

APPENDIX

HELPFUL TOOLS:

https://www.hushmail.com/
https://www.enigmail.net/home/index.php
http://tails.boum.org
https://www.torproject.org/download/download-easy.html
http://www.trisquare.us/
http://www.cypherpunks.ca/otr/otr-codecon.pdf

OTP RESOURCES:

https://babkjl.wordpress.com/2012/03/18/one-time-pad-cryptography/
http://users.telenet.be/d.rijmenants/en/otp.htm