# GUIDE TO SAFELY USING SATPHONES V2.0

At Fasila we believe the capacity to tell a good story is a precursor to social change. But we know many people lack the security to tell their own stories without fear of reprisal. Because of that, in addition to communication and storytelling training, we produce content related to digital and physical safety. It takes more than the knowledge of tools and techniques to tell a good story. Individuals need to feel safe in their own communities.

Whether you are looking for someone to teach you or your team how to tell stories, or how to be safe telling them, Fasila will show you how.

For more information about Fasila visit: https://fasila-inc.com

Fasila

## Table of Contents

# Overview

Satellite phones, also known as sat phones, are becoming popular communication tools. In areas with low access to traditional communication tools or where communications have been cut off, humanitarian workers, first responders, journalists, and in some situations activists may need sat phones to reach the outside world.

However, using a sat phone presents particular risks.

For example, when you depend on this complex technology it is impossible to know exactly how your communication is being monitored. Today local, regional, and national governments as well as intelligence agencies, hackers, and commercial agencies all may be able to monitor your communications. Also, governments have a variety of reasons for restricting or banning sat phones, and those governments may search for people using them. This guide will assist you to maintain a low profile and improve your chances to evade detection and monitoring of your activities. Although using sat phones comes with proven danger, the guide will decrease your risks in highly controlled areas.

If you have a situation that is not included in this guide, please let us know! You can send recommendations and comments on the guide via our contact form here: https://www.fasila-inc.com/contact, however, this is not a good place to send questions if you find yourself at risk.

***NOTE:*** *This is the second version of this guide, updated in July 2022. A previous guide was printed under the auspices of Small World News (SWN), an entity that predates Fasila. Currently Fasila holds all of the intellectual property previously held by SWN.*

# 1.0 What Is a satellite phone?

A satellite telephone, satellite phone, or sat phone is a type of mobile phone that connects to orbiting satellites instead of terrestrial cell sites. They provide similar functionality to terrestrial mobile telephones; voice, short messaging service and low-bandwidth internet access are supported through most systems.

Sat phones, like mobile phones, are complicated radio transmitters that function by transmitting data via a radio signal, in addition they have a receiver which receives data such as the voice of the individual on the other end of the line. Sat phones send the signal to a satellite in orbit around the earth. The satellite then broadcasts the signal back to earth, to a "Ground Earth Station," or GES. From the GES the signal is sent via the normal terrestrial phone system or Internet to its destination, the receiver of the call. The GES acts as a gateway between your sat phone, traditional cellular mobile phone networks, landline networks, and other satphones.

Transmitting information to the satellite in orbit is the "uplink." Receiving information from the satellite is the "downlink." This information can be data or voice. A phone's signal can be intercepted anytime it has an active connection with the satellite: during the uplink or the downlink.

***SECURITY NOTE:*** *If you communicate with someone outside the sat phone's service provider network your communications are subject to any observation happening on the other user. Communicating with other sat phones from the same service provider is much safer. Even this method is not entirely secure, but following these basic steps will limit your risks.*

This guide provides the techniques necessary to increase your safety, but is not a guarantee of secure communications-since the original guide was written the security risks of sat phone communications have only increased. For example vulnerabilities have been found in all the known encryption protocols used by satellite communications providers, and recent events in Ukraine have demonstrated that new vulnerabilities continue to be found.

# Operating a Satellite Phone

# 2.0

Sat phones may look like very large mobile phones, but they differ in some key areas.
The activation process is relatively similar, while the connection process poses notable differences.

Understand each step of operating a sat phone in order to effectively identify possible risks and challenges you may face, particularly in hostile environments.

## 2.1 Activation

Sat phones require activated SIM cards and must have a plan associated with the SIM card. The plan may be prepaid or postpaid. If prepaid the phone must have minutes associated with the SIM card. Minutes can be paid for and added online or directly from the phone by submitting scratch card codes via SMS.

See **Section 7.2** for details on adding credit to an iSatphone 2 sat phone.

## 2.2 Connection

Unlike mobile phones, sat phones do not connect automatically to their network. Sat phones speak directly to one or more satellites in orbit far overhead.

To obtain a signal you must stand still, aim the phone's antenna towards the sky, and wait for the phone to locate a signal. Your phone will first obtain a GPS location fix, then it will connect to the network. This process may take over a minute.

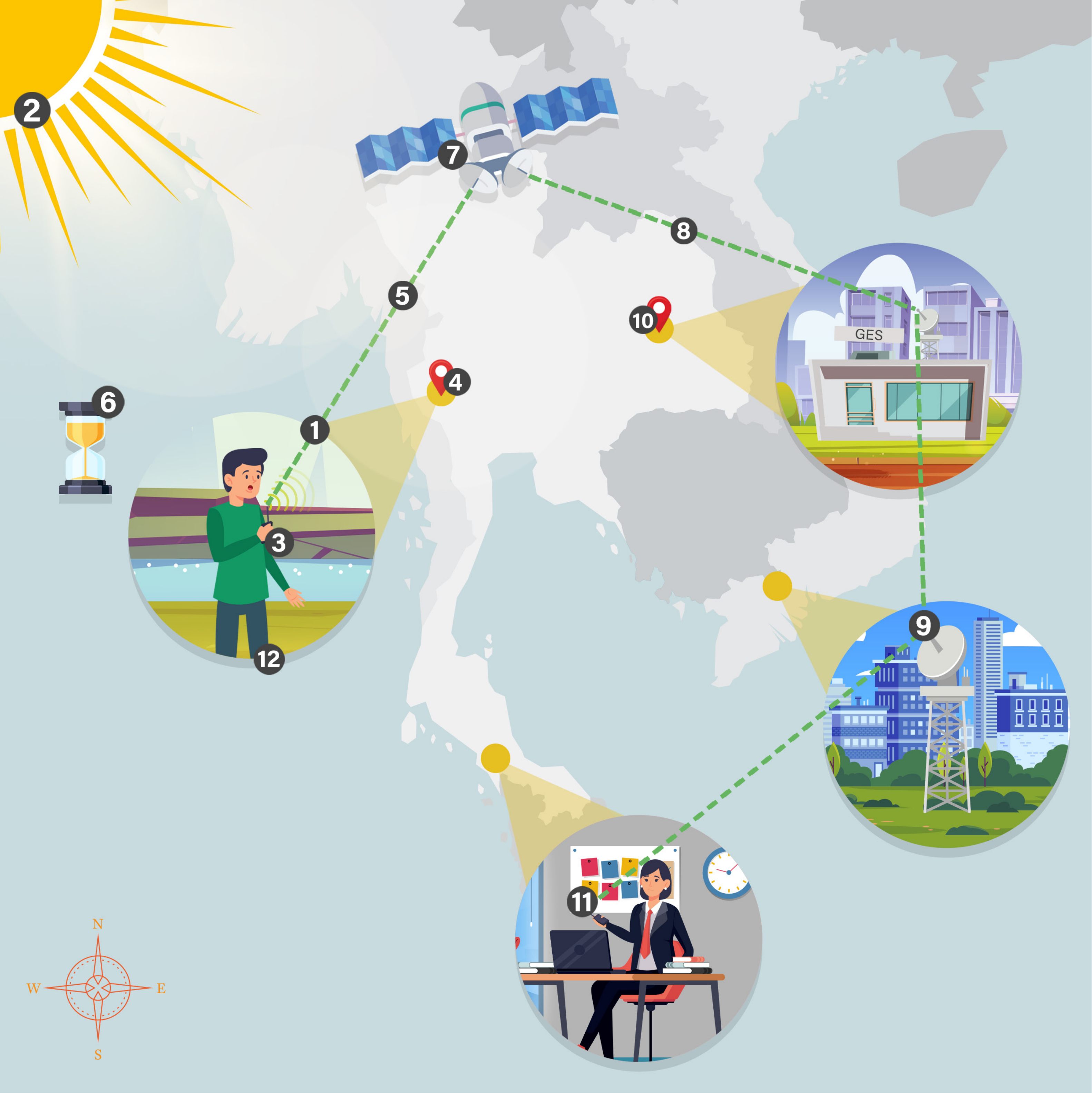
While you are waiting for the phone to connect you may be observed by the authorities. In **Section 4.2** we will discuss steps you can take to disguise your phone. Following those steps may reduce your risk.

***SECURITY NOTE:*** *The time needed to connect with the network is the first major security risk. In order to obtain a signal, the phone must be "deployed" meaning the antenna must be in the on position. Unlike a cellular mobile phone, a sat phone will not receive calls simply by being turned on. Sat phones are not able to communicate unless the user intentionally connects to the network. This makes it difficult to have unscheduled calls with other sat phone users. Therefore, satellite phones should not be depended on for urgent or emergency communications.*

## 2.3 Using a Satellite Phone, a Walkthrough

This is a complete overview for the steps involved in making a phone call or sending a message from a sat phone.

1. Turn on the phone.
2. Find a clear view of the sky.
3. Engage the antenna to look for a signal.
4. The phone obtains a GPS fix and logs its GPS location.
5. The phone connects to the satellite network.
6. Make a call or send an SMS/email.
7. The phone uplinks to the satellite.
8. The satellite downlinks with a Ground Earth Station (GES).
9. The GES transmits the information to the intended recipient.
10. The GES records the phone's GPS locations while transmitting.
11. Complete the call or SMS/email.
12. The phone logs the phone number called/texted and the length of the call.
13. Close your antenna.
14. Limit your risk. (Delete your call record and texts, clear your outbox, etc.)
15. Turn off and store the phone.


2
7
8
5
10
4
6
1
GES
3
12
9
11
N
W
E
S

13
14
15

# Known Risks from Satellite Phones

# 3.0

Satellite phones pose a variety of risks to users. Most risks, such as confiscation, are no different from the risks posed by your mobile phone. The device creates records in normal usage that can be used to locate and identify the individuals you communicate with.

Although mobile phones can also be intercepted and tracked, the mechanisms for intercepting and tracking sat phone calls are somewhat different, as are the resources necessary. This section identifies the similarities and differences, and what can be done about them.

## 3.1 Phone Confiscation

In many cases, you and your colleagues will be your own worst enemies. If the phone is confiscated or stolen it may provide a treasure trove of unintended data and information. Information such as who you contact most, when, and for how long can be found in the call log. Your contacts' phone numbers may be found in the phonebook. Perhaps most importantly, specific, detailed information might be taken from your text conversations and emails with others. There are many technical risks with satellite communication, but the most likely risk is user-generated. These risks are often overlooked because they are primarily caused by normal operation. While modern cellphones have encryption enabled by default, sat phones do not have the same protections against confiscation and forensic examination.

In some countries checkpoints and searches are regular occurrences. Sometimes these checkpoints are well-known, but they can be random or you may be unfamiliar with them if you don't know the area. If your phone is confiscated at a checkpoint your phone's features such as the call log, phone book, and sent folder can endanger your life and the lives of others.

These features help you keep your contacts handy, but they also provide an easily accessed record for the authorities to track your calls, even if they do not have access to your transmissions.

When a file on a computer is deleted, it is not completely destroyed and may be "reconstructed" without further measures. It is also possible your sat phone's logs can be reconstructed from the sat phone. Deleting information is not a complete failsafe, but will make it harder for authorities to access information on a confiscated phone.

### 3.1.1 Call Log

By default, your phone will keep a log of everyone you have called. Be sure to delete this every time you make a phone call. Any number you have left in the log will be at risk if your phone is confiscated. It may be suspicious to have an empty call log, but will have less impact on your colleagues.

### 3.1.2 Sent Folder

Similar to the call log, your phone will maintain a list of SMS and email messages sent from the phone. Be sure to delete these after each message is delivered.

### 3.1.3 Phonebook

Your phonebook also provides a list of potential suspects for the authorities. Any person listed in the phonebook will be at risk if your phone is confiscated. It may be suspicious to have an empty phonebook, but will have less impact on your colleagues. You may be tempted to put in pseudonyms for contacts, but it is still worth considering if the country code or area code of the contact will by itself be incriminating for you or reveal sensitive information.

## 3.2 Signals Interception and Tracking

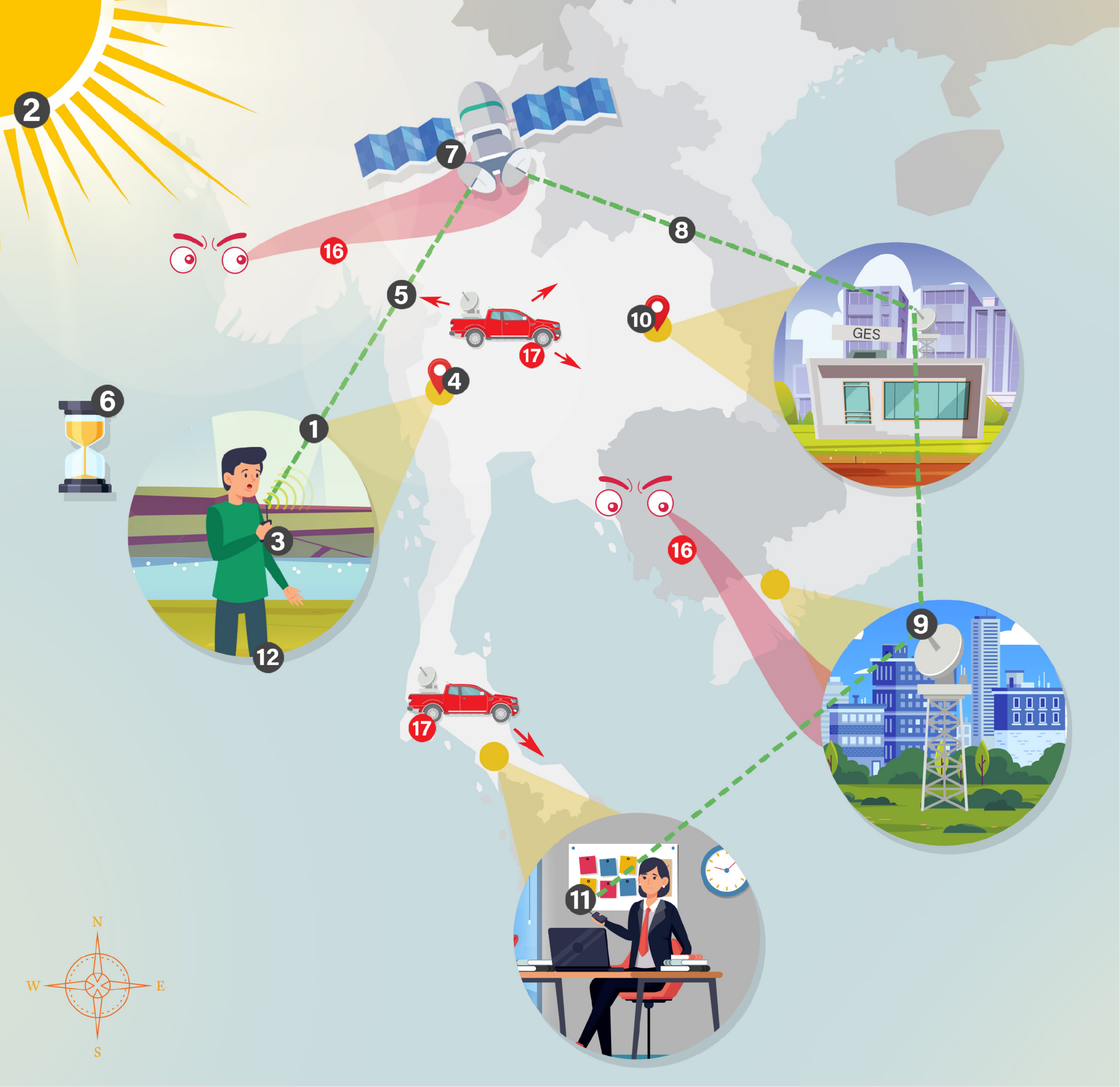
All phones are radio transmitters. Sat phones send a radio signal to a satellite in orbit around the earth. The satellite then broadcasts the signal back to earth, to a "Ground Earth Station," or GES. From the GES the signal goes through the internet to its destination, the receiver of the call. A sat phone's signal can be intercepted anytime it has an active connection with the satellite: during the uplink or the downlink, when the satellite is sending the receiver's voice back down to you.

Depending on the equipment available to the authorities, there are different potential risks for signal interception, outlined in this section.

The diagram below annotates the areas where your sat phone signal may be intercepted and your communications may be surveilled.

16 Your communications may be observed by anyone with access to the satellite or GES records, including the service provider, police and military, and possibly bad actors with access to interception technology. **See Section 1.0** for more details.

17 Your communications may be intercepted by the military or police if they have ad vanced technology to do ground-based tracking. They may also be able to triangu late your location. This can be done without you or the service provider being aware.



## 3.2.1 Radio Signals Transmissions

Satellite communications use radio signals to transmit information. These transmissions can be triangulated with affordable, even homemade tools. Triangulation uses two or more signal receivers to determine the location of a radio signal transmitter. A signal receiver is any radio that can receive as well as transmit a signal. Your phone, for example, is a receiver as well as a transmitter. Many countries have access to advanced technology that allows them to receive signals and triangulate the signals location. The location is determined by the receiver based on the axes of the angles of receivers. Triangulation can also be done with one mobile receiver. Highly developed countries with advanced technical capabilities are likely to have this capacity, however less developed states and even non-state actors may be able to develop the capacity, or it may be provided by an ally.

For these reasons, keep all transmissions as short as possible. Our recommendation is to keep transmissions under three minutes, while other experts recommend less than ten minutes. It's impossible to know the absolute minimum time necessary in all circumstances. The limiting factors are just too varied–technical capacity, geography or terrain, and preparedness of those trying to intercept are all factors–therefore always keep your transmission as short as possible.

In some cases the authorities may have the proper equipment to "listen in" on your transmissions, however this requires highly advanced and sophisticated technology. Review Section 5.4 for tips on how to communicate more safely if you suspect your calls are being monitored. Although voice decryption has been demonstrated in near real-time with some protocols, it's also possible to record calls and decrypt later, which may pose additional risks in the future.

### 3.2.2 GPS Location Transmissions

Satellite communications require a GPS location for optimal functionality. GPS means Global Positioning System. Your GPS location gives exact coordinates for authorities to find your location. This provides the potential for an individual using any satellite device to be located with exact coordinates. Your location may be logged at the service provider's Ground Earth Station (GES). The GES data may be accessible to many different groups including local or nearby governments, shareholders, local service partners and anyone who is able to hack the GES security systems.

If the authorities possess the correct technology, or have the specific encryption and transmission codes of your sat phone model they may use your phone's GPS coordinates to locate and detain you.

## 3.3 Encryption Decoding

Satellite transmissions are encrypted, but many governments are capable of defeating the encryption used by these phones. Standard encryption may deter detection and monitoring but cannot guarantee security.

***SECURITY UPDATE 2022:*** *Numerous providers of interception solutions claim to be able to break the encryption on sat phones from all providers. At this time, we do not recommend depending on or expecting your satellite transmissions to be protected by the encryption afforded by the device. The GMR-1 and GMR-2 encryption protocols were entirely broken in 2017. Although Inmarsat, for example, claims that they have already accounted for this issue, they have provided no public explanation for their claims. While these claims have not been verified, the lack of publicly available information either proving or disproving these claims should be sufficient to cause sat phone users to think twice about what they say over a sat phone connection.*

Satellite communications are vulnerable to prying ears and eyes, who may review voice, message, and data transmissions. Even if the necessary equipment and capability to break the encryption may not be available to the authorities in your area they may be able to break it over time. If the authorities can intercept your transmissions, and they are capable of recording the signals, it is likely they will eventually break the signal's encryption and review the content of your calls or messages.

*Given the potential for authorities to obtain such equipment, you should think very carefully before you share personal, life threatening, or other critical information via satellite. see Section 5.4* ***Deceive by Speaking in Codes*** *for suggestions on how to deter the authorities from understanding the content of your call or message.*

# 4.0 Basic Precautions for Limiting Risk

Sat phones are closed technology, and not easy to modify. Because of this it is impossible to have completely secure communications with a sat phone. There is always the possibility that your call can be recorded and listened to, even at a much later time. As mentioned in the previous section, at the time of publication in 2022 numerous retailers claim to provide solutions for intercepting and decrypting transmissions.

However, the precautions provided in this section can be used with any sat phone to increase your safety and decrease the risk of observation or detention by authorities.

The recommendations below are not without their own challenges. Replacing a sat phone SIM is much more difficult than getting a new SIM for your mobile phone. If you don't have a backup for your records, deleting them may bring additional complications. In particular, if you live in a country where mere ownership of a sat phone is illegal or suspicious, these recommendations may protect your contacts, but not necessarily yourself.

## 4.1 Delete All Records

Do not save communications information on the sat phone. Although security services may obtain calling records through other means, do not make it easy for them. Even without names a list of phone numbers, cellular or satellite, for authorities to track and locate could be catastrophic. Each phone manufacturer has a different system, so become familiar with the steps to delete records on your phone as soon as possible.

> ***NOTE:*** *See Section 7.0 for specific steps to make the Inmarsat iSatphone 2 safer.*

When communicating with individuals who may be threatened or under surveillance, be sure to maintain their information in a safe and secure location. Always store this information in a secure fashion.

## 4.2 Disguise Your Phone

When using the phone for calls, do not leave it out in the open. Satellite phones require larger antennas for communicating with satellites in orbit and resemble large, outdated mobile phones, which may draw unwanted attention. Always pair with a headset, so it will appear you are using the local cellular network not making a satellite call. Using a Bluetooth headset will make it easier to disguise the phone, however there are additional security risks, listed in Section 7.5.

Keep the phone hidden at all times and disguise it if you have time. Place the phone in a location with a good angle toward the satellite's position, but disguise its physical location as much as possible.  Put the phone inside an open bag, or behind some bushes. This may be difficult as the phone needs a clear view of the sky. If possible experiment in a safe location to see how you can evade observation without interfering with the phone's connection.

## 4.3 Destroy Your SIM Card and Phone

If your phone is confiscated, the SIM card will provide information that can be used against you and your colleagues. Keep the SIM card out of the phone so it can be quickly destroyed. If possible destroying your phone may further limit your risk, however it's more important to follow the precautions in **Sections 4.1** and **4.2** than  attempt to avoid detection by the authorities.

Destroying a sat phone can be quite challenging. These devices are built to be rugged and withstand extreme temperatures. Although you may be able to break the antenna without much effort, this only prevents the device from communicating, while the data you want to destroy is left safe inside the device. You may need to use tools such as a hammer or electric saw, drive over the phone with a vehicle, or drop it several times from a tall height.

Once the casing is cracked proceed to destroy the internal parts and distribute them in different locations so that reconstruction is difficult.

***SECURITY NOTE:*** *This is an extreme method for protecting yourself and your colleagues. The method is also irreversible, however depending on your level of risk tolerance and the perceived threat against you, destruction of the device may be your best course of action.*

# Using your Satellite Phone More Safely

# 5.0

The previous section outlined basic precautions you can take with any sat phone. This section explains specific techniques for using your sat phone more safely in each of the primary uses, making voice calls and sending SMS or email messages.

## 5.1 Voice Calls

Voice calls are a very risky method for communicating via satellite. When making a call, be sure to keep the call as short as possible, due to the potential for interception of your phone's radio signals, or GPS location.

### 5.1.1 Making Phone Calls

Authorities may use your phone's radio signals to detect your position within less than three minutes. As their techniques become more sophisticated they may be able to locate a sat phone even more quickly. In some cases authorities may be able to listen in to your phone call, by intercepting its radio signals transmissions. Authorities may tap the phone at the other end, if they have access to the service provider. **See Section 3.2.1** for more information about radio signals transmissions.

The longer you remain on the line, the greater opportunity you provide the authorities to find your exact position via your phone's GPS location.

### 5.1.2 Interviews and Longer Calls

As noted in **Section 5.1.1**, if you are worried about your calls being monitored or triangulated it is important to keep your call as short as possible. Sometimes that's not possible, especially if you are in an area that is difficult to reach and you are doing an interview with a member of the media or providing an update about necessary aid.

When making an interview, be sure the interviewer is clear on your situation and do not remain on the line longer than you feel safe. It is best to keep your call under three minutes. Whether it's an interview or an update to colleagues, prepare your comments beforehand, and be clear that you will not discuss items outside your planned communication.

When making a voice call to communicate with a colleague or coordinate with other activists, remember to **Speak in Codes**. This is important in order to **Deceive** anyone who may be listening in, or may break your phone's encryption.

**Speaking in Codes** and using common phrases that have a double meaning may keep you or others safe, although you may never know that your conversation was being monitored. Utilize common phrases, rather than special words you would not otherwise discuss.

**Delete** your phone's call log. There is nothing worse than creating an indexed archive of information that is waiting for the authorities. If you fail to do this, you will put others at risk and may increase the potential threat to yourself if your phone is confiscated.

## 5.2 SMS

**SMS** is a highly convenient method of sending a message. SMS is delivered via email, where your phone number is attached to a carrier specific server address, such as example@text.phonecarrier.com.

Despite manufacturer claims, SMS does not provide secure encryption. Do not transmit sensitive information via SMS unless you are willing to have it read by the authorities. If the SMS is intercepted, it is likely to be recorded and the encryption broken at a later date, if not immediately.

SMS may take less time than a voice call, so the risk of intercepting the SMS Radio Signal or exploiting the phone's GPS location may be less than with voice. However it is more likely the content of your message will be retrievable by the authorities, if your transmission is intercepted.

**Deceive** unwanted observers through the use of code phrases and terms with double meaning.
**Delete** SMS from your phone's sent folder. There is nothing worse than creating an indexed archive of information that is waiting for the authorities to review in the event you are detained.

## 5.3 EMAIL

Email can be sent via any satellite phone,  but is delivered via the same protocols as SMS, and restricted to approximately 160 characters.

You may decide to use the email feature rather than SMS because you expect email to be more secure. This is incorrect. Email sent from your sat phone does not provide the same protection as email sent via computer or mobile data plans.

Computer and mobile internet both provide the opportunity to use additional security tools. Email can be sent by computer or mobile over an HTTPS connection that is far more difficult to intercept. On some mobile phones and all computers Tor can be used to anonymize your computers traffic and hide your identity and location. If at all possible use a secure internet connection to communicate, not a sat phone.

Because, like SMS, an email transmission may take less time than a voice call, the risk of intercepting the message via the radio signal or exploiting the phone's GPS Location may be less than with voice. However it is more likely the content of your message will be retrievable by the authorities, if your transmission is intercepted.

**Deceive** unwanted observers through the use of code phrases and terms with double meaning.
**Delete** email from your phone's sent folder. There is nothing worse than creating an indexed archive of information that is waiting for the authorities to review in the event you are detained.

## 5.4 Deceive by Speaking in Code

In cases where you are communicating with collaborators, fellow activists, etc. hide your true intentions. Use codes, discuss common subjects that you are likely to share, yet have double meanings. Do not discuss your intentions directly.

**EXAMPLE:**

Use memorable phrases and terms with double meanings, or use familiar subject matter such as specific religious verses. For example, use a term to indicate authorities such as "uncle."

When checking with a contact to first determine whether the contact is safe from authorities, one might ask,  "Has your uncle come to town?" Yes may indicate it is not a good time to talk, no indicates it is safe.

This enables further codes, your contact could say "My uncle was here, but he left, I'm going to be busy for the next few days," indicating it's inadvisable for you to try and reach your contact in the near future.

Additionally "My Uncle was here, he reminded me that the family reunion is happening soon," could indicate the authorities may be planning to interrogate you or your other colleagues soon.

You may also want to consider codes that don't have such a direct relationship, where the combination of subjects discussed provides information. Also providing false or misleading information, such as a location, can confuse anyone who may be listening in.

For example "Did I tell you about my cousin's wedding that is coming up? She is marrying a very good man from Aleppo." In this case the term "wedding" and "very good man" could be operative phrases, where "wedding" indicates the authorities may be looking for you soon, and "very good man" indicates the specific security service involved.  Using another phrase such as "wealthy merchant" will indicate a different office.

Covering your intentions may save your life or others.

In many cases a simple code might be sufficient, but for ongoing, regular communication, or communication with a group, it may be necessary to have at least a rudimentary codebook.

**SECURITY NOTE:** *Codes, code making, and codebreaking are all extremely technical skills that require experience and practical knowledge to implement at more than a basic level. This guide recommends that you focus on a small number of innocent words or phrases that you can substitute in normal conversation that will alert the intended recipient but sound like nothing more than small talk to anyone else who might be listening.*

The table below demonstrates how you might combine words that likely appear as innocent small talk, in order to share a hidden, coded message. **DO NOT USE THIS TABLE OR ANY PORTION OF IT IN DEVELOPING YOUR OWN CODES.**

| Original Word | Code | Example |
|---|---|---|
| electricity | mangoes | I have no **mangoes** today, can you help? Do you have any? |
| home | temple | I will be going to the **temple** later, can you meet me? |
| arrested | angered | Did you hear that Jon **angered** his mom today? |
| checkpoint | traffic jam | There is a bad **traffic jam** in my area, do you know another way home? |
| safe | cool | No worries, everything is **cool**. My **uncle** and I made it through the **traffic jam** and we are at the **temple**. |
| friend | uncle | Did you remember my **uncle**? He **angered** our **neighbor** yesterday! |

As you can hopefully see, there are ways to stack codes, using multiple coded words in a single sentence. More complicated codes may be difficult to remember or deliver effectively. You may want to write down what you want to say before calling your contact, and those who are aware of your code should be prepared to take down the message with their own notebook. Another option is to send these messages by SMS.

Depending on the level of organization in your group or team, you may want to create a lot of codes, or keep them to a few crucial points, or swap only a few crucial terms. Take this example and play around with it with your contacts. Highly organized groups engaged in regular communication and at high risk of surveillance may want to add a shifting element to the codes, changing them based on the day of the week.

For example:

| Monday | | | Tuesday | | | Wednesday | | |
|---|---|---|---|---|---|---|---|---|
| Original Word | Code | Example | Original Word | Code | Example | Original Word | Code | Example |
| electricity | mangoes | I have no mangoes today, can you help? Do you have any? | electricity | apples | I have no apples today, can you help? Do you have any? | electricity | pencils | I have no pencils, can you help? Do you have any? |
| home | temple | I will be going to the temple later, can you meet me? | | | | | | |
| arrested | angered | Did you hear that Jon angered his mom today? | | | | | | |
| check point | traffic jam | There is a bad traffic jam in my area, do you know another way home? | | | | | | |
| safe | cool | No worries, everything is cool. My uncle and I made it through the traffic jam and we are at the temple. | | | | | | |
| | | Did you remember my uncle? He angered our neighbor yesterday! | | | | | | |
| friend | uncle | A funny thing happened today, I saw chickens outside the temple, can you imagine? | | | | | | |
| police | chickens | | | | | | | |

# Choosing What Brand You Should Use

6.0

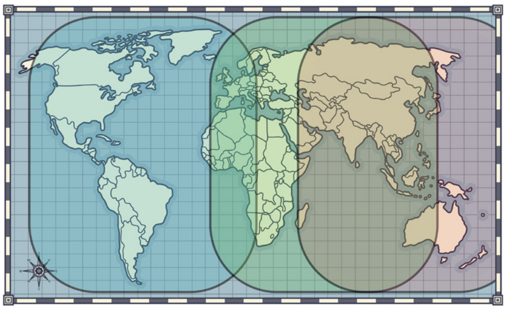
All sat phones are not equal. Each brand has its limitations, though as will be explained, we recommend not using Thuraya phones if you can avoid them. That warning aside, the previous sections will still provide the best practices to follow to limit your risk.

There are a variety of satellite communications service providers, including Thuraya, Inmarsat, Iridium, and GlobalStar. Others such as MSV, ICO, Teledesic are currently non-operational or do not provide consumer services.

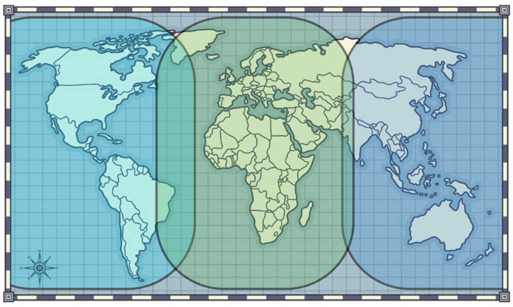
Keep in mind that there are legal constraints on satellite communications that vary from country to country. In some countries such as India satellite phones are highly regulated and mostly illegal. It's your responsibility to be apprised of the constraints on using satellite phones in the country you are operating in.

## 6.1 How to Choose

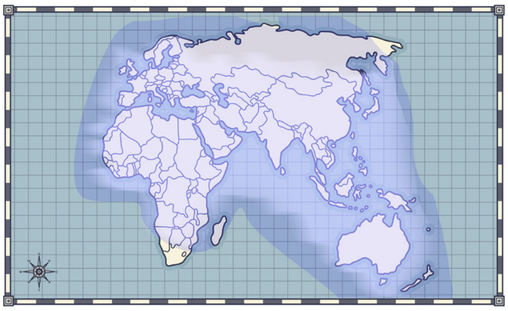
There are a variety of factors to consider when choosing a sat phone: connectivity in your region, availability, reliability, overall security, your needed features, and risk factors related to your intended use. You should consider all of these when choosing a sat phone. First and foremost you'll want to check which brands have connectivity in your region.



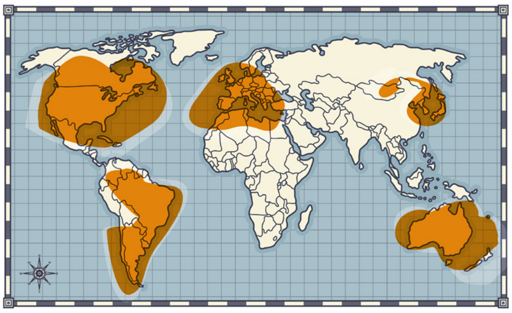
Iridium Coverage



Inmarsat Coverage



Thuraya Coverage



Globalstar Coverage

As is hopefully clear from these maps, Iridium and Inmarsat have the most extensive coverage, while Globalstar and Thuraya are much more limited. That doesn't necessarily mean that Iridium or Inmarsat are your best choices.

Your choice should be first informed by whether or not the satellite company even provides coverage in your area. Next it's important to consider the other factors mentioned at the beginning of this section, each of which will be discussed in detail.

### 6.1.1 Availability

When thinking about availability there are some important questions to answer first: Can sat phones be purchased in your region or country?

Sat phones cannot usually be obtained at a moment's notice, not only are they highly regulated, they're not generally in high demand. Unlike buying a new mobile phone which can be managed at any number of different shops, satellite phones typically need to be bought online or at specialized distributors. It may be illegal to have a satellite phone shipped to your country. Educate yourself, do not rely on the retailer to inform you, and it may be advisable to use a VPN or an anonymous, public computer to do your research.

*If it is illegal to purchase or obtain a sat phone in your country, how will you get one? Are there limiting factors that reduce the options available to you?*

### 6.1.2 Reliability

If you're lucky enough to have the option to select from a couple of different sat phones, reliability is a good next measure. The safest, most secure device is useless if there's no coverage available in your area.

Reliability can typically be judged by a few simple factors.

- Age of the model
- Coverage area
- Battery life
- Ongoing technical support and updates

Typically newer model devices are more expensive, but will be easier to find replacement parts and obtain technical support if needed. The youngest model devices tend to have the best support and battery life. However buying a cutting edge device is not without its own risks. These may be potentially serious such as unidentified security flaws in features such as the device's implementation of encryption or less serious such as firmware or battery life issues.

Be sure to read the reviews and discuss with a satellite phone sales representative if possible. Confirm the device will provide coverage in your area of implementation and doesn't have any known flaws that may dissuade you from selecting it.

### 6.1.3

### 6.1.3 Overall Security

Overall security is a challenging concept to define, and in many cases even harder to determine. We might consider the company's track record of vulnerabilities and responses to the public when security flaws are identified. Another method may be to look at the company's primary or largest clients, for example Iridium has large contracts with the United States military, therefore it might be safe to assume they provide the best encryption and overall security available on the market.

However, security is not only about criminals or other adversaries actively compromising your communications outside of a legal framework. Whatever company you trust with your communications has direct access to the content of your communications. This includes voice calls, text messages, and in the case of some devices data transfers such as emails or social media posts.

It's important to examine the company you are using and ask what factors may cause them to share your information with a third party, such as a government agency, but this may also include extra-legal pressures, depending on your work and location. If you are concerned about the United States government accessing your communications you might not want to use Iridium.

***SECURITY NOTE:*** *If the United States government is interested in accessing your communications, there's likely little you can do to mitigate this, aside from not communicating over satellite or really any other electronic means. Iridium is a US company with many reasons to cooperate with requests submitted via proper legal channels. Although Inmarsat is headquartered in the United Kingdom, the long history of cooperation between the US and UK, particularly on issues of national security and intelligence suggest there's an equally high likelihood of cooperation from Inmarsat, assuming the proper legal channels are followed.*

### 6.1.4 Needed Features

In addition to checking reviews and checking factors such as reliability and security, it may be very helpful to speak with those who have experience with the sat phone you are considering. Beyond these considerations lies the realm of personal responsibility–only you can determine what is the best combination of features for your individual needs.

Take a few minutes to draft a rudimentary communication plan. Who do you need to reach and when? Do they have access to a working phone line such as a mobile or landline device? How will you make sure they can reach you when needed, and vice versa?

Next turn this rudimentary plan into a checklist. This list should give you a fairly accurate overview of the features needed for your communication plan to have a chance of succeeding.

### 6.1.5 Personal Risk Factors

Based on our research, although no sat phone is truly safe and secure from determined authorities, we have found that Thuraya, in particular, is unsafe, and should be avoided at all cost.
We are recommending Inmarsat's iSatphone 2 for ease of use, availability, and its recent rise as an entry-level device used by many journalists and activists across the Middle East.

## 6.2 Why Use Inmarsat's iSatphone 2?

Why do we believe the iSatphone 2 is safer than Thuraya, and relatively as safe as other brands? While Thuraya is definitely compromised, other services may be compromised as well.
The contents of this guide will assist you  to maintain the greatest amount of safety possible, despite the serious risks posed by satellite communications technology.

Aside from Thuraya the two most popular and experienced companies providing satellite communications are Iridium and Inmarsat. If secure communications are your number one priority and you are not concerned about surveillance by the United States or its allies then you should stick with Iridium. However, in most cases the additional levels of protection professed by Iridium are outweighed by the relatively similar security provided by Inmarsat devices, at a significantly lower cost. Over the past ten years, since releasing the iSatphone Pro, Inmarsat has seen its market share increase significantly, especially among journalists and humanitarian workers.

At the time of this guide's original publication in January 2012, there were no known exploits of Inmarsat phones by the Syrian authorities. As a company based in the United Kingdom, there are legal constraints preventing Inmarsat from providing records to the Syrian Government. At the time of publication there were no accounts of Inmarsat phone users detained due to the operation of an Inmarsat phone.

***SECURITY NOTE:*** *All satellite phones pose significant potential risks to the user, based on the very real potential for interception of the transmissions and location information.*

6.3

***SECURITY UPDATE 2022:** At the time of publication in 2022 the best information available strongly suggests that there is no reliable encryption available on any satellite phone provider. The best protections afforded to end users rely on the legal whims of corporations and their countries of incorporation. For example, as in the case of Inmarsat, legal constraints prevented Inmarsat from providing records to the Syrian government–assuming they would have considered it. At the same time, although uncertain, the likelihood of Inmarsat providing records to the UK government or even the United States may be considered far more plausible.*

## 6.3 Why Not Thuraya?

### 6.3.1 Background

Thuraya became one of the more popular satellite communications companies, due to its affordable products and broad functionality, particularly in the Middle East. Throughout 2011 the popularity of Thuraya began to decrease, due to the ease with which governments are able to block or intercept Thuraya. Blocking was first seen over 6 months in 2006 as the Libyan government engaged in massive jamming of the service from within its territory. Likely due to Thuraya's popularity in the Middle East the United States targeted this provider in particular for interception and encryption decoding.

### 6.3.2 Thuraya's Problems

In 2011 Syrian activists alleged the Syrian government compromised Thuraya's network security. It is believed that Rami Makhlouf controls the Syrian subsidiary of Thuraya. Activists believe he obtained access to Thuraya's decryption codes and other records and provided these to the Syrian regime. Detained activists have later reported hearing recordings of conversations they made over sat phones. We have been unable to determine if the recording happened by interception of an uplink. It seems likely the activists were communicating with someone on a local service provider that was tapped by the authorities.

According to Strategy Page, in 2003, "Thuraya recently announced that while the phones did transmit the GPS location periodically (to insure a good satellite signal), the information was sent in encrypted form and only someone with access to the codes, or with powerful decryption capabilities, could get the location information (of the phone broadcasting the information)."

***SECURITY NOTE:** In February 2012, two German researchers demonstrated the capability to decode the GMR-1 and GMR-2 encryption standards. These standards are not used by all satellite phones, however Thuraya and Inmarsat both use this standard. The method used is fairly technical, however the potential is now documented and it is likely that governments will soon begin obtaining the necessary technology.*

It is also documented that the US, and possibly Indian authorities were able to listen in on conversations between individuals using Thuraya phones, ahead of the terrorist attacks across Mumbai in 2008, "Officials say one of the phones recovered was a Thuraya satellite phone. "Once we have the number we will be able to know everyone who was called and where the calls were made from," one former intelligence officer says."

Based on this information, we recommend activists avoid using Thuraya phones in any circumstance.

## 6.4 Helpful Accessories

In addition to the techniques and precautions provided throughout this guide,
there are accessories that you may find helpful. Keep in mind that off-brand accessories may not have the same reliability as original equipment, and pay attention to any security precautions provided by the guide.

Some of these accessories may come with your sat phone, be sure to keep them handy!

### 6.4.1 Extra Batteries

This accessory should be obvious, but it can be easily overlooked, especially as many smart phones no longer have the ability to swap batteries. Sat phones can use a lot of juice and unfortunately their batteries and power economy have not had the same advances seen in smartphones over the last few years.

It's important to remember that battery life varies with use and your mileage may vary.
For example, the iSatphone 2 advertises a talk time of 8 hours on a single charge, and 160 hours of standby time. That may be enough for you, but if you are working in areas without reliable electricity for more than a day or two, you may want to bring additional batteries. Inmarsat's official replacement battery also boasts 8 hours of talk time, but only 100 hours of standby time. Do some basic math to figure out how many batteries you need and consider increasing that number by at least one.

### 6.4.2 Car Charger

Depending on the sat phone you purchase and where you purchase it, there may be a car charger included. A car charger is an important accessory for a variety of reasons. First and foremost, as mentioned in **Section 6.4.1** it's always good to have backup power for your sat phone. Secondly, a car charger can be useful if you intend to use a car-mounted antenna, or want to charge your phone with DC power from a variety of sources.

> ***NOTE:*** *If you will use a car-mounted antenna (**See Section 6.4.4**) be sure that you have a car charger with two USB ports so that you can power the phone and the antenna at the same time.*

### 6.4.3 Bluetooth Headset

Using a bluetooth headset can be a great idea for a variety of reasons. First of all, sat phones require a very specific positioning and are bulky and may be annoying to hold for a long time. Having a bluetooth headset connected means you can set the phone in a stable position and have the freedom to walk around unencumbered and without worrying that you will lose your signal.

If you are using a car-mounted antenna (**see Section 6.4.4**) the sat phone is usually mounted in a specific location. In this circumstance a bluetooth headset may be much easier or more effective than using a wired headset or the device's speakerphone capacity.

There are a variety of risks when using a bluetooth headset, if you decide to use one be sure to read **Section 7.6 Using a Bluetooth Headset to Reduce Suspicion.**

## 6.4.4 Car-mounted Antenna

Car-mounted antennas are generally shaped like small domes and have a strong magnet on the bottom in order to attach the device to a car or boat.

Because of the way sat phones work, necessitating a constant line-of-sight to the satellite, it is very difficult to use a sat phone on its own while in a moving vehicle. Car-mounted antennas provide the sat phone with an omnidirectional antenna that is affixed to the top of the vehicle and connected to the sat phone by a wire.

***NOTE:*** *You don't need to be in a car to use one of these antennas. Because of the low-profile shape and omnidirectional nature, they may be less obvious than standing in an open space with a sat phone pointed at the sky. When using a car-mounted antenna you can speak from a hidden place or inside a building, so long as it's within the reach of the wire that came with your antenna.*

**SECURITY NOTE:** *If the wire breaks or is lost you will not be able to connect your sat phone to the car-mounted antenna. Remember to purchase one or more additional wires to connect the phone and the antenna. If you intend to use the antenna from a distance, make sure you get a wire long enough for your intended placement.*

## 6.4.5 Cables

Your sat phone needs a variety of cables to use all of its intended functions. Exactly what cables your sat phone requires and what functions they provide may vary slightly depending on the manufacturer.

The device may use a standard microUSB cable for some functions. Other functions such as connecting the phone to an external antenna require a unique cable.  Although you can use many cigarette adapters with USB ports, the iSatphone 2 typically comes with a specific wired microUSB to cigarette port cable.

Think hard about how you will use your device and make sure you have all the necessary cables. In some cases you may want multiple versions of the same cable. The standard-length antenna cable is generally sufficient for connecting your device to a vehicle-based antenna, but if you want to use the device from inside a building or under other cover you may wish to purchase the longest available antenna cable–in some cases you may be able to get a cable that is 10 or 12 meters in length.

### 6.4.6 Docking Station

If you're using a vehicle antenna you'll most likely receive a docking station as part of the kit. This enables you to mount the phone on your dash or windshield while running a static cable out the window to the antenna.

There are a variety of other circumstances where you might want a docking station, in particular to make the device easily accessible, immobile, and hands-free. If you typically mount your smartphone when driving, consider getting a mount made specifically for your sat phone of choice.

### 6.4.7 Inmarsat IsatPhone 2 External Vehicular Antenna Kit

If you'll be moving often and need to maintain a connection while on the go, the Inmarsat External Vehicular Antenna Kit is a great option. It comes with all the parts you need to get your Inmarsat 2 up and running and on the go right out of the box. Remember if you intend to use the antenna in other setups this is totally doable, but you may want to consider buying a longer length antenna cable.

# How to Improve
## The Safety of an iSatphone 2

# 7.0

In many cases, you and your colleagues will be your own worst enemies. Although there are many technical risks with satellite communication, the most likely risk is user-generated. These risks are often overlooked because they are primarily caused by normal user operation.

In the case of repressive states, phone features such as the call log, phone book, and sent folder can endanger your life and the lives of others. These features keep your contacts handy, but also provide a record for the authorities to track your calls, even if they do not have access to your transmissions.

These directions will make the iSatphone 2 safer and help you avoid the risks mentioned in this guide.

## 7.1 Lock Your Phone

To prevent unwanted eyes from examining your phone, turn on the admin code,  and pin request functions. This may be found by accessing **Menu > Settings > Security.**

When choosing number codes **DO NOT** choose codes with all the same number, or easy combinations such as 1111 or 1122. By default the admin code is 123456, this code must be 6 digits. If you misdial your code you can re-enter an unlimited number of times.

The SIM pin by default is 8888, this code must be between 4 and 8 digits. The SIM pin 2 by default is 9999, this code must be between 4 and 8 digits. If the SIM codes are entered incorrectly three times your SIM will only be unlocked by obtaining the PUK code.

## 7.2 Add Phone Credit Remotely

To add credit to your iSatphone 2 you need to first purchase credit. This can be done at a number of websites, such as http://satphonecity.com

To check your phone’s balance, make a call to this code: *106#

To add balance to your phone from a voucher, enter the following code: *101*VoucherNumber#

For example: *101*123456789#

## 7.3 Clear Your Call Log

By default, your phone will keep a log of everyone you have called. Be sure to delete this every time you make a phone call. Any number you have left in the log will be at risk if the phone is confiscated. It may be suspicious to have an empty call log, but will have less impact on your colleagues.

Delete the **Call Log** by accessing **Menu** > **Call Log** > **Options** > **Clear all**

## 7.4 Delete Your Sent Folder

Similar to the call log, your phone will maintain a list of SMS and email message sent from the phone. Be sure to Delete these after every delivery.

**Delete** SMS and email messages by accessing **Menu** > **Messaging** > **Sent** > **Options** > **Delete all messages**

## 7.5 Delete Your Phonebook

Your phonebook also provides the authorities a checklist if it lists your colleagues' phone numbers. Any number left in the phonebook will be at risk if the phone is confiscated. It may be suspicious to have an empty phonebook, but it will have less impact on your colleagues.

Delete your **Phonebook** by accessing **Menu** > **Contacts** > **Phonebook** > **Delete all**

You can **Delete** any contacts stored on the SIM card by accessing **Menu** > **Contacts** > **Sim Contacts**

## 7.6 Use a Bluetooth Headset to Minimize Suspicion

Do not leave the phone out in the open. Keep it hidden at all times and consider disguising the phone.

When using the phone for calls, if at all possible, pair with a headset. It will appear you are using the local cellular network, not making a satellite call. Place the phone in a location with a good angle toward the satellite, but disguise the phone's physical location. Using a bluetooth headset will make it easier to disguise the phone, but may result in other risks listed below.

Activate the phones' bluetooth capacity by accessing **Menu** > **Settings** > **Bluetooth** > **Paired Devices** > **Options** > **Search for devices**

When "discoverable" your Bluetooth signal will be visible to devices detecting Bluetooth transmissions within 10 meters. Always keep your Bluetooth non-discoverable. **NEVER** connect your sat phone to an unknown Bluetooth device. Always use a headset with a "push-to-sync" button. The Bluetooth signal switches randomly among 79 radio frequencies, 1600 times per second, making it very difficult to intercept the transmission.

***SECURITY NOTE:*** *There is equipment on the market that will enable anyone to monitor, record, and decrypt Bluetooth audio transmissions in real time. The likelihood of authorities to have access to this equipment is unknown, though not impossible. If you are not currently being monitored, it will be difficult for the authorities to observe you, based on your Bluetooth transmissions alone.*

## 7.7 Disable Your Phone and Keep Your SIM Card Secure

The iSatphone 2 will not connect with the network, and should not transmit GPS or other signals when the antenna is not deployed. Remove the SIM card and keep it with you, this will make it easy to destroy in the event of confiscation. Always close the antenna to **disable** the phone when not in use

# Satellite Phone Use and Scenarios

## 8.0

This final section of the guide poses some scenarios in which you might need to use a satellite phone, and provides specific suggestions and cautions, or dos and don’ts. These are only theoretical and should not be expected to cover every eventuality in your situation, so please refer to them with caution.

First a refresher on the relevant functionality of sat phones. Keep in mind that sat phones can only make or receive calls when turned on, with the antenna activated, and properly sighted with a clear view of the sky and angled toward the satellite’s position.

The most common reason for using a sat phone is to communicate with your home or office while in a remote location which has no communications infrastructure, whether mobile connectivity, landlines, or internet access. This may be the common state of affairs, such as in extremely remote areas such as parts of the Sahara and Amazon, or Antarctica.

In other cases the lack of infrastructure may be sudden, due to natural disasters such as hurricanes or floods, or due to a government shutdown of communications or due to undersea cables being severed. Although some individuals may be prepared for this type of incident, more often than not there will be a lag between the incident and the availability of satellite communications.

When two or more individuals are in contact entirely via satellite communication timing and proper scheduling is essential. Another solution is to set up external antennas. If you have a properly placed 360 vehicle antenna, in a window with a clear view of the sky in the appropriate direction, or on the roof, and a sufficiently long cable, your phone can be inside, well out of sight of the satellite, but you will still be connected, and able to send or receive calls.

In addition to these situations sat phones are sometimes used in more challenging circumstances, such as the war in Syria as mentioned in an earlier section. They may be used by individuals,such as humanitarian workers or journalists, trapped in a remote area where no information is coming out. They may be used by individuals whose primary communications such as mobile phone and email have been targeted by a rogue faction of a security force or intelligence agency.

## 8.1 Calling Home While Remote

What needs to be kept in mind when using your sat phone as the main point of contact with your home or office?

Consider the story of Lin and May. May is in the field shooting a nature documentary in a rural part of Laos. At their main office in New York City, Lin receives several sudden calls from one of their clients and needs to speak with May as soon as possible. Forgetting that he cannot reach her if her sat phone is not activated and connected to the satellite Lin calls May several times without success, becoming very frustrated. Eventually Lin sends her a frantic, frustrated text message. Three hours later, May calls Lin at their previously appointed time, having received the text message just before, once her phone connected to the satellite.

Make sure those you are in contact with understand that you will not be able to speak with them at any given moment. Since your phone must be deployed and properly aimed, callers at home will not be able to call you on a moment's notice.

Establish a schedule for speaking with each particular contact that you must speak with on a regular basis. Every twelve or eight hours is usually sufficient as a maximum. If you're in a particularly dangerous or risky environment, this schedule should be tighter. If it's only possible to schedule a daily call you may consider scheduling a "missed call check-in" such as: If the call home doesn't happen, and your contact doesn't hear from you after 12 hours, initiate your security plan.

In this scenario, the challenges are fairly low, and generally unrelated to your sat phone. Things to remember:

- Keep your schedule clear
- Keep your sat phone battery and extra batteries charged
  Check your schedule for the day–will you be able to get a connection at the appointed time?
- If not, reschedule with your contacts
- Set your sat phone plan to auto-renew if you run out of credit, or be sure to add credit
  If you are on the non-sat phone end of a call, remember you can send a text message that will be received as soon as the sat phone is connected to the satellite.

## 8.2 Calling Between Two or More Sat Phones

Contact between two sat phones can be extremely frustrating, and may necessitate a lot of patience on at least one of the two individuals. Imagine you and a colleague are in two different locations responding to the same disaster, if you're calling them, but they haven't yet deployed their phone, or they are having trouble getting a connection, you're not going to connect. How long should you wait to give up? It depends on your situation, some considerations:

- Are you in a safe location?
- Is it tolerable to be outside for a long period of time?
- Do you have other deadlines?

Let’s look at another story about Lin and May, this time out in the field together, documenting an aid organization providing assistance to monsoon survivors in an area of India where cellular communications have been knocked out. In order to cover as much as possible in the few days they have on site, May and Lin decide to split their efforts, each traveling to a different town. Fortunately they brought two sat phones, but only two. May suggested they send their assistant Devi ahead to check the terrain and other affected areas, but soon realize without a third sat phone Devi will be unable to communicate findings unless with May or Lin. Given they are in India where sat phones are tightly controlled due to concerns about terrorism and insurgents, it isn’t possible to get another sat phone without a long wait and a difficult bureaucratic process.

While they are in the field, despite having highly recommended sat phones, they encounter a number of challenges. May is in an area with poor access to the sky in the appropriate geographic orientation to reach the required satellite. All while Lin and Devi are sent ahead together to scout a few locations at once, requiring them to be on the road almost constantly. Despite having a set check-in time, neither is able to access their sat phones at the proper time. May cannot establish a connection until fifteen minutes after the appropriate time, heading first to an area of town which has an appropriate vantage on the sky. Lin and Devi are stuck on the road, in a heavy traffic jam but do their best to get a connection, however they cannot reach May. By the time May reaches the appropriate vantage, the traffic jam is moving again and Devi cannot manage to maintain their connection while the vehicle is moving. To make matters worse, May’s battery is low and  there is no electricity accessible in either area. By accident all the extra batteries were left with Devi and Lin and May’s phone dies before she can reach them. Additionally, police in the area begin to take notice of Lin and Devi standing on the side of the road with a sat phone, but fortunately Devi has a written approval from the Department of Telecommunication. Eventually they convince the policeman that they are not a threat, explaining that they are documenting the aid work in monsoon-affected towns and villages. By the time they reach the last town on their list, having been unable to reach May, they head back to their basecamp to regroup.

When they regroup at their client’s basecamp the next day batteries are split between the two teams, and they agree to check their connection at least ten minutes before a scheduled call, whenever possible. Additionally they make a backup plan to send messages via the sat phones SMS function if they are not able to connect by phone.

There are some key practices that you might implement to reduce the challenges to connecting with one or more colleagues all using sat phones. In the above situation, the team had prior approval to use a sat phone, otherwise they would most likely be, fined, deported, and possibly arrested. First of all keep in mind those recommendations in Section 8.1 they all apply here as well. Additional things to remember:

- First ensure that this type of communication will be sufficient, unless your team have arrived on site with multiple sat phones, it may be difficult to find sufficient devices for your needs, at least for several days.
- If possible, set up an external antenna, such as those meant for vehicles, this way you may be able to set up your sat phone so that it is always accessing a connection via the antenna, even if you are inside working on something else.
- If you don’t have access to an external antenna, a bluetooth headset may provide a suit able stand-in. However your mobility will be more limited as you must stay within range of the sat phone’s bluetooth signal, approximately ten meters.

- Consider using both a bluetooth headset and an external antenna for even longer range
- Remember you can send a message or email from your sat phone which will be delivered when your contact connects their phone–suggest a few times that you will reconnect to your sat phone to connect directly. Consider making this a regular policy if concurrent connectivity continues to be a problem.

## 8.3 Calling Under Surveillance

There are a number of circumstances where you might find your communications under surveillance, especially if you are using a sat phone. In those cases you need to be more cautious with how and when you use these devices. Additionally in some areas, such as India, satellite phones are tightly controlled by the government and virtually outlawed, due to fears of terrorism or insurgent activities. In these types of situations, simply possessing a sat phone may be sufficient to put you at great risk.

The final story from May, Lin, and Devi is their most challenging one yet. They've been asked to document the work being done in a remote refugee camp that's been recently established, and does not have reliable cellular communication or internet access. Additionally, there have been multiple threats against the refugees, both from the government of their home country who accuse them of being affiliated with an ongoing insurgency and the local people living around the camp who see them as taking away from the already meager resources.

There may not be reliable electricity either, but this time Devi remembers to distribute the batteries evenly between both teams, as well as providing them headsets and one vehicle-mounted antenna to more easily access the satellite network while on the road. Unfortunately their budget only accounted for one device.

On their second day Lin gets lost near the border and uses his sat phone to call Devi and request advice. While he is speaking to her he is surrounded by soldiers, having not realized he is in a restricted area. He quickly realizes that they are concerned about his sat phone and various recording equipment he is transporting. The soldiers take his phone, disconnecting his call with Devi. Fortunately Devi knows that May is working at the camp, not too far from Lin's location and because she has the vehicle with their mounted antenna Devi has no trouble reaching her.

May quickly reroutes her plan for the day and heads to the border area to look for the military base and hopefully find Lin. One of their client's local leads goes with May, because he has a good relationship with the local commander. When they arrive the situation is quickly diffused as the commander attempts to explain the situation. While drinking tea and waiting for Lin to be brought to them the commander even shows May, and the local staff person how they are using newly supplied technology to track satellite phones in real-time. Understanding that May get a good connection, and is seen by some nearby protesters who mistake him for an agitator and believe him to be planning something against their gathering.

Several surround Lin and begin shouting in the local dialect, shaking their fists and one throws a rock at him. He realizes they are concerned about his phone and quickly hangs up the call as he dodges more rocks. He is only saved by the local staff person who jumps out of the car and after a few minutes is able to calm the crowd.

and Lin are foreigners, the commander brags about their capabilities which he claims can lock on to and track satellite transmissions “within minutes.”

With Lin returned safe and sound they load up their gear and head back to where they are staying. Along the way they run into another traffic jam near the refugee camp. Local people are staging a protest near the refugee camp. Devi has heard about the protest and, worried about Lin and May, she calls them to check on their situation. When Lin answers he is standing outside of his vehicle to get a good connection, and is seen by some nearby protesters who mistake him for an agitator and believe him to be planning something against their gathering.

Several surround Lin and begin shouting in the local dialect, shaking their fists and one throws a rock at him. He realizes they are concerned about his phone and quickly hangs up the call as he dodges more rocks. He is only saved by the local staff person who jumps out of the car and after a few minutes is able to calm the crowd.

Hopefully you can see how in some circumstances using a sat phone publicly can be quite a risk, even if you are not doing anything improper or undesired by people on the ground, whether we are talking about government security forces such as police, military, or border patrol, or getting in the middle of a conflict between local civilians.

Most if not all of the suggestions in **Section 8.1** and **Section 8.2** would have benefited the team in this situation. As you can also see, they learned from previous mistakes. What else can you do to reduce your risks?

- Confirm the local regulations for sat phone usage, especially if you are working undercover, for example in a conflict zone, tracking migrations, or other investigative or human rights work that may put you in conflict with local people or authorities
- Make a security plan aimed at reducing your risks, check and double-check this plan. How/When will you use the sat phone? What is your escape plan if a member of your team gets in trouble?
- Use a vehicle-mounted antenna if this makes sense. It can stand out, but it also provides near-constant connectivity except in very tight quarters such as ravines or urban areas where the angle to the sky may be blocked.
- Consider using the vehicle-mounted antenna as a stationary antenna if you will be in one location for a while, this enables the sat phone to work inside and may provide a clearer connection as well.
- Keep calls short, consider communicating primarily by SMS. We recommend you keep your voice calls no more than three minutes, and other experts recommend under one minute, the higher the risk you’re in, the shorter your call should be. Your main goal is to keep the communication as short as possible.
- The content of SMS may be easier to intercept than voice calls, so use at your discretion, consider whether the risk of the message being read is higher than the chance you may be tracked and detained, or worse if you are in an active conflict area, you may be targeted by ordnance such as mortars, rockets, or missiles. Always try to send your SMS and emails in codes as mentioned in **Section 5.4**

## 8.4 Communications Cheat Sheet

Lastly, here's a brief breakdown of some situations where you may need to use a sat phone, and what considerations your team should make before implementing sat phone communications.

Do you have:

important information to share but internet and phones are disconnected?

- call someone outside the disconnected area
- call another satellite phone
- send an email/text

important information to share from a remote area that has no regular communications?

- in this case satellite phones may be more common or well-known
- sat phones could be harder to hide
- but possibly they may be less noticed

important information to share but your regular communications are being tracked?

- plan to be mobile
- be more concerned about the content of your words
- may be more dangerous to communicate by text
- Never communicate from the same spot twice.

***Security Note:*** *Never depend on someone who only has access to a sat phones as your primary emergency contact. Sat phones can provide challenges in the best of circumstances to even the most highly trained individuals. Remember they cannot even receive calls if they are not both activated and connected to the satellite.*

If you have a situation that is not included in this guide, please let us know! You can send recommendations and comments on the guide via our contact form here: https://www.fasila-inc.com/contact, however, this is not a good place to send questions if you find yourself at risk.