Operational Security (OPSEC) For The Radio Amateur.

Chris Warren July 16, 2019 No Comments on Operational Security (OPSEC) For The Radio Amateur.

It seems so innocuous.

Have you ever spotted an impressive antenna on someone's house and thought, *"wow, now there's a kickass setup!"* Or maybe you have a neighbor who goes for a one hour jog at the same time every day. What about that house up your street that is very nicely kept but no one is ever seen there?

What can we conclude about these people?

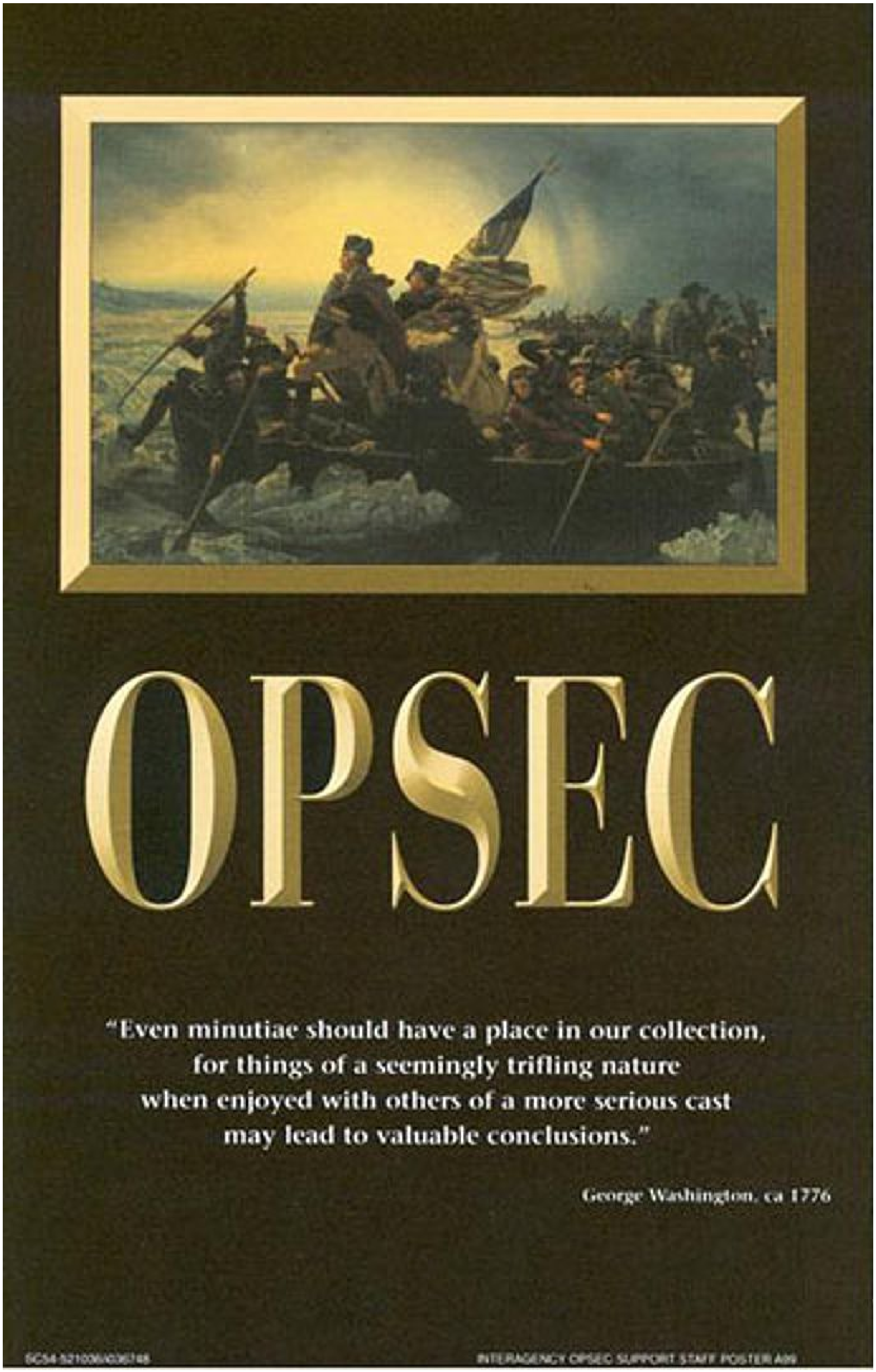
When you really think about it, there is quite a bit you can learn about others by observing normal, everyday situations and activities. One does not need to spy or stalk or do anything unethical or illegal to suss out what others are doing and make accurate conclusions about their activities and lifestyle.

This of course is a two-way street. Others can determine a lot about you based solely on your outward behavior. That's why radio amateurs especially need to be mindful of operational security, or OPSEC.

What is OPSEC?

Operational security is a big deal in the government and the military, and like all things government/military, they make it really complicated. If you google "opsec" you'll get endless pages of detailed analyses. For the average off grid ham, we can reduce it down to a short statement: *OPSEC is making sure those who do not need to know your business do not know your business.*

In corporate lingo, OPSEC is referred to as *competitive intelligence*. The principle is basically the same: Glean information about your competitors from readily available sources, then use it against them. Some large companies actually encourage employees to send in tips.



OPSEC

"Even minutiae should have a place in our collection,
for things of a seemingly trifling nature
when enjoyed with others of a more serious cast
may lead to valuable conclusions."

George Washington, ca 1776

SC54-521008/036748

INTERAGENCY OPSEC SUPPORT STAFF POSTER A99

The bottom line is that OPSEC is information, and information has value to people who may not wish you well. What do you say about yourself by just living your ordinary life?

Unintended OPSEC violations.

I was on 2-meter simplex a while back and had a nice chat with a guy who in the course of a ten minute QSO revealed that he A) is a software engineer with an advanced degree who works long hours, B) lives alone in a quiet neighborhood, C) owns a lot of high end electronics, D) drives an expensive luxury car. He was about 20 miles from me, so his signal was being heard over a large area.

It was just casual chatter, so what's the big deal? Hmmm let's see: He's a well educated software engineer with a luxury car and a lot of electronic "toys," so he probably has money. His house is empty most of the time. A simple lookup of his call sign would reveal an address in an affluent town. From there you can figure out what a less than honest person might be inclined to do.

I gleaned all this information from one simple on-air exchange, the kind many hams engage in every day. He probably did not even realize that he was exposing himself to trouble.

Normalcy bias.

Many OPSEC violations originate from a psychological condition called *normalcy bias*. Normalcy bias is when someone underestimates or may be in complete denial of the possibility of a serious situation. In layman's terms, it's an *"it can't happen to me"* attitude. I'm sure you've seen videos of natural disasters taken by people who should have been running in the opposite direction. That's normalcy bias. Or maybe you don't think much about oversharing personal details about yourself on the local repeater because, well, what's the likelihood that some villain will hear you and go through the effort to track down at your address? That's normalcy bias too.

If you are or have been in the American military, you may have never heard the term "normalcy bias" but you probably know what it is. You've been trained and trained and trained to assume nothing and always anticipate the worst. For everyone else, do whatever you must to rid yourselves of normalcy bias. At best, it encourages OPSEC violations. At worst, it will kill you.

Plugging the holes.

Short of forfeiting your radio license and becoming an antisocial recluse there isn't any way to completely eliminate all OPSEC liabilities. There are some easy things you can do.

Do not reveal specific details about your personal schedule or habits:

YES: "I coach my son's volleyball team." **NO**: "I coach my son's volleyball team every Monday & Wednesday from 5-7 pm."

YES: "I'm running an errand". **NO**: "I'll be at the mall for at least a few hours."

Be mindful of how you respond to queries. Neighbors and others may make comments about things you can't really hide, such as antennas and solar panels:

YES: "I'm an amateur radio hobbyist. It's a pastime I really enjoy." **NO**: "I have a comprehensive worldwide communications system and off grid power. When SHTF, I'll be ready while you poor bastards sit in the dark!"

Have some awareness of what others may observe on/around your property:

YES: Before discarding the box from that expensive electronic device, turn it inside out to hide the label. **NO**: Just leave it at the curb intact so everyone knows you just got a $3000 TV set.

YES: Make use of concealment such as landscaping, window blinds, fences, etc. **NO**: Unnecessarily leave the garage door open all weekend as if it were a showroom for your power tools.

Educate your allies.

One of the biggest OPSEC violations may be the people closest to you! Teenagers love to blab, especially on social media. Family and friends may talk, with kind intentions, about your radio and off grid capabilities. Let them know you're really flattered but you prefer it be kept within a tight circle. Explain when SHTF, there will be more resources for them if the whole world does not know what you have. Play to their selfish side.

OPSEC and the internet/social media.

Wow, entire books could be written about operational security and the internet. It's going off topic for this blog, so I'll keep it simple: Do not post anything on the internet that you would not want plastered on a billboard along a major interstate highway! This includes photos.

You may not have noticed my amateur radio call sign does not appear anywhere on this website. I do not reveal my exact QTH, not even the state I live in. When I respond to reader emails or comment on other blogs, it's always through a VPN. All of this is done on purpose. I don't worry about my name too much because it's so common that googling it will lead nosey people into a vast sea of Chris Warrens (I know because I've tried it). I also have the added benefit of a androgynous name.

It's not that I think no one will ever find me, it's that I've deliberately made myself as obscure as possible. The internet is a great resource, but be very circumspect and guarded about what you say. Don't make it easy to find you.

OPSEC and radio clubs, groups, EMCOMM.

Any time you get involved with an amateur radio club or group, or participate in emergency communications (EMCOMM) activities, you are to to some extent lowering your OPSEC. Your capabilities, or lack of them, will be an open book and you don't always know who you are dealing with.

If you are involved with EMCOMM, then you'll be also be dealing with the government at least indirectly. It's one thing if your radio buddies know what you've got. It's quite another when the government knows! In a December 2018 *Off Grid Ham* article I related a personal story where my county disaster agency invited me to join their EMCOMM group. The application included a lengthy list of questions asking about my power generation capabilities, off road vehicles, special equipment & tools, technical skills, and other information that I considered very invasive and off-putting. I did not like the idea of being on some local bureaucrat's list of people with skills and cool stuff, so I declined the invite.

The advice I gave then is still valid: I'm not trying to scare anyone away from what could be a great experience. I simply want radio amateurs to examine very closely what they disclose about themselves versus the benefits of being in the group. Who will have access to your information? Why do they even need to know?

Physical security.

Physical security is what you need when OPSEC fails. This is not the venue to get deep into it, but take a good look at your door locks, exterior lighting, and other security features on your property. Think about physical security when you're not at home. I very strongly suggest getting proper, professional self defense firearms training and purchasing a gun (do it in that order). Do not take gun "training" from your uncle Ed who was in the military 30 years ago or your boy/girl friend who likes to go plinking at the range every now and then. I absolutely do carry a gun and believe every eligible adult should too. If you are not willing or able to carry a gun, then make other plans for your safety that go well beyond simply dialing 911 and hoping for the best. *"When seconds count, the police are minutes away"*.

What we learned today.

- In simple terms, operational security (OPSEC) is making sure those who do not need to know your business do not know your business.
- Any ordinary personal trait, habit, or activity has the potential to be an OPSEC violation: What time you leave for work, what kind of car you drive, how you dress, etc.
- Most OPSEC violations are unintended. It's almost impossible to be 100% operationally secure.
- Normalcy bias is a psychological condition that can lead to committing OPSEC violations.
- Educate those close to you about the importance of OPSEC.
- Be especially mindful of what you say on line.
- Involvement in an amateur radio club or EMCOMM group presents unique OPSEC challenges.
- Make accommodations for your physical security.