



2D MARINE DIVISION

Unit, Personal and Family Readiness

OPSEC for Families

Presentation materials provided by OSPA (www.opsecprofessionals.org)



Your loved one has the training, leadership and equipment needed to perform the mission and come back home to you.

***But did you know that you're
half of the team?***

The military provides certain training and equipment designed to keep your loved one safe.

You may not know it, but you play a critical role in your loved one's safety just by protecting what you know about their day to day and operations.

This is known as OPSEC.





What is OPSEC?



Operations Security (or OPSEC), for a family member, is simply denying any enemies access to information. The information that you have **ALREADY**, such as mission, vehicle capabilities, location and tactics are considered intelligence by enemies of the US. By not allowing the information that you have to get out, you help make sure that your Marine or Sailor can maintain the upper hand.



What OPSEC is:

- Denying any useful information to the enemy
- A mindset, a way of thinking
- Applied to web pages, blogs, emails
- A standard that can be applied to any situation



What OPSEC is NOT:

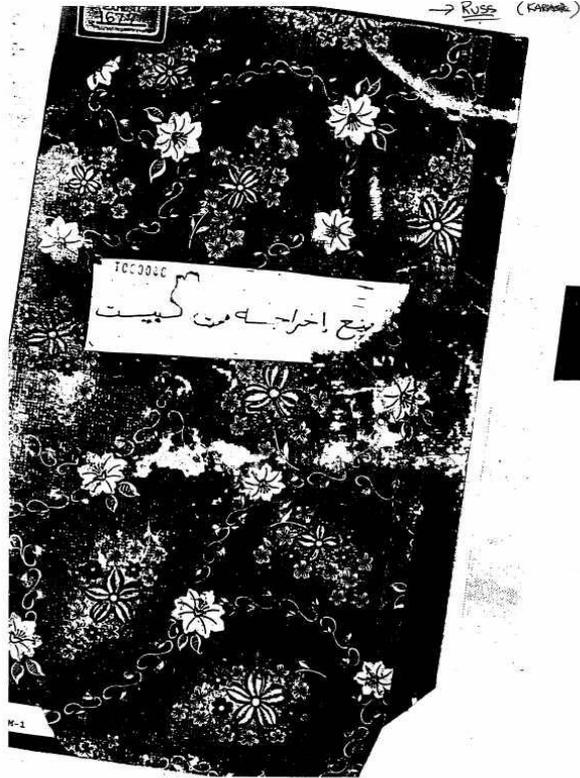
- A collection of specific rules to cover every possible situation



Every piece of information is like a piece of a puzzle.

The type of vehicle your Marine drives might not seem like important intelligence, but when combined with other pieces of information, such as location, unit name, unit structure and mission, an enemy can begin to build a profile of the organization.





GOVERNMENT
EXHIBIT
1677-7
(10)

UK/BM-1 TRANSLATION

IT IS FORBIDDEN TO REMOVE THIS FROM THE HOUSE

Embassy bombings
of ~~the~~ Southern District Court
New York City Attorney General's
Office
Entered as evidence in trial of Abuja

This manual was captured in a home raid in Iraq, and is only one of countless copies.

According to this manual, 80% of military intelligence can be collected from legal sources, including websites, blogs, newspapers and online.



Who would try to get information from a spouse or parent?

- Foreign intelligence
- US citizens
- Terrorists
- Criminals
- Coalition partners
- Computer hackers

Military families have been the targets of attempts to gain intelligence through active means, such as fraud, overhearing public conversations, computer hacking or false friendships, as well as passive means such as monitoring a blog, military-spouse or -family themed chat rooms and personal websites.



“On the internet, nobody knows you’re a dog”

Readers of your blog or forum posting might appear very friendly. They might claim to be stationed near your spouse, or to have a loved one deployed as well. No matter the technique, the underlying goal may be to make you comfortable enough to reveal things that you otherwise would not.



“On the Internet, nobody knows you’re a dog.”



What information are they looking for?

- Military movement information, such as dates and locations
- Unit issues, especially morale or dissatisfaction
- Security issues, such as tactics or defenses
- Equipment issues
- Specific location of unit
- Pictures of successful attacks (both ours and theirs)
- Pictures that could be interpreted differently than intended

Equipment issues: In OIF III, a well meaning spouse sent a letter that got leaked detailing vehicle armor, unit mission and specific vehicle capabilities on mission. The unit responded appropriately before the information became a threat, but it could have been far worse.



If you were an enemy, could you use this picture?

Perception is OPSEC's worst enemy.



In reality, these two Iraqis were caught allegedly looting gasoline from a burning building, and the 12 year old pictured was quickly released. No matter how you describe the picture on your personal website or blog, the picture can often be used against the US!

It's not that you should avoid the web altogether. You're going to be proud of your Marine or Sailor, and will probably want to talk to others about them. It is important, though, to understand the risks associated with any public medium and adjust accordingly.



What you can do

- Ensure that the information posted has no significant value to the enemy
- Always assume that the enemy is reading what you're writing
- Be careful about discussing information in public settings (Clubs, airports, gyms, grocery stores)
- Avoid publically (online or real life) speculation about future missions (“they’ll probably start a build-up next”)



What you can do

Be especially careful to safeguard “indicators”, pieces of information that provide clues about future activities:

- Railhead dates
- Increase in field exercises
- Ceremonies
- POV storage
- Increase in financial activity, such as wills and power of attorneys





A note on telephones

Remember that cordless phones and cell phones are NOT completely secure! Anything you say is transmitted over the airwaves and can be intercepted.



Same is true with landline phones! Lines can be crossed or intentionally intercepted!



The bottom line

Think like the “bad guy” before you post something online or have a public conversation.

Coordinate with your unit's Family Readiness Officer and have pictures screened and posted to the unit's "Official" Family Readiness website.

You CAN protect your loved ones by protecting the information that you know.





Questions?

