**3.2 What’s your Operational Environment?**

**Intro:** In this section, participants will continue to develop skills in risk assessment and planning, this time focusing on specific local or contextual threats to information security and mobile security.

**Timing:** 1+ hours, depending the time available and need for focus on this issue. Some operational environments are more threatening than others.

**Equipment Needed:**

* Whiteboard or large sheets of paper and markers to document discussion and contributions from participants.
* Copies of the [Risk Assessment Preparation Worksheet: Operational Environment](http://www.google.com/url?q=https%3A%2F%2Fdocs.google.com%2Fdocument%2Fd%2F1MAb1DXYL6IYC-zNZsBtVKBPOuHhbVLfdze6kn7qxdnA%2Fedit%3Fhl%3Den_US).

**Content Outline and Main Topics:**

1. **Discussion/Instruction (10 minutes):** What is an operational environment?
2. **Instruction (10 minutes):** Defining operational security. Discuss the various considerations as per SaferMobile’s [Guide to Mobile Security Risk Assessment](http://www.mobileactive.org/risk-assessment).
3. **Instruction/Discussion (10 minutes):** Do you trust your technology providers?
4. **Exercise (30 minutes):** Assessing operational security risks. Work through the various aspects of operational security for a given situation (either real-life or scenario-based).
5. [Risk Assessment Preparation Worksheet: Operational Environment](https://docs.google.com/document/d/1MAb1DXYL6IYC-zNZsBtVKBPOuHhbVLfdze6kn7qxdnA/edit?hl=en_US).

**Objectives/Expected Outcomes:**

* Participants will strengthen their new skills and knowledge in mobile security by integrating them with local knowledge about their operational environment.
* This exercise will build the critical skills for risk assessment and planning and help participants think systematically about their environment, resources, how the complex “mechanics” of information security operate, and what role mobiles and their security play in the larger area of overall information security.
* Participants will complete the [Risk Assessment Preparation Worksheet: Operational Environment](https://docs.google.com/document/d/1MAb1DXYL6IYC-zNZsBtVKBPOuHhbVLfdze6kn7qxdnA/edit?hl=en_US), in preparation for developing their own risk assessment and mobile security policy in Unit 5.

**Additional Resources for Trainers and Participants:**

[Guide to Mobile Security Risk Assessment](http://www.mobileactive.org/risk-assessment)

[Mobile Risk Primer](http://www.mobileactive.org/howtos/mobile-security-risks)

**Content**

**1. Discussion/Instruction (10 minutes)**:

Broadly speaking, your operational environment can include *any* factors that allow or prevent you from operating to meet your individual or organizational goals, as well as what can define those goals. Environmental factors can be anything at the national, community, or local level that affects your ability to conduct your work safely, effectively, and legally. International considerations can also become factors, but for the purpose of this exercise, have participants focus on the local and national operating environment, as most factors are based on state-based regulations, laws, and social, cultural, and political variations.

Your operational environment can change rapidly, especially with regard to technology. A service or activity that previously hasn’t been a target of security forces can easily become one.

**2. Instruction (10 minutes)**: Defining operational security.

Based on your experience, you and your colleagues likely have a sense of the threats you face. Consider the following:

1. Your work in the context of a given society and culture.

* **Political and human rights**. Are political and human rights respected in the country that you are working in? If you are working in a location that restricts civil liberties, even the smallest project could be high risk. For additional assistance considering the political and human rights context of your project, see [this Freedom House map](http://www.freedomhouse.org/template.cfm?page=363&year=2011).
* **Reputation.** Connections to other organizations could both provide protection and increase your risks. Among your team, are some of you more at risk than others? Are you part of a larger network? Do you have foreign partners? Does your association with these entities increase the likelihood of risk?
* **Issue and controversy**. How are the issues that you work on seen by the population in which you work? Do you have support from the general population? Are the issues you work on particularly controversial?

2. The legality of your tactics and tools.

* **Are the tactics you are using considered legal where you are working?** If they are illegal, your risk increases considerably.  (For the record: We do not condone or support any illegal activities.)
* **Are the security tools that you are using legal or illegal where you are working?** For example, is it legal to encrypt your communications?

3. Technological vulnerabilities and threat.

* **Mobile networks and devices**. Are you aware of the general vulnerabilities of mobile communication and whether your phone calls and messages are easily threatened? Do you know how mobile networks operate and what information your MNO knows about you?
* **Availability and reliability of service**. Are you able to use your mobile device for communication in all locations where you will be working? Is service generally reliable or often disrupted, intentionally or unintentionally?
* **Policy and oversight**. What are the policies regulating whether and how governments and other entities can intercept your communications and access your communication records?
* **Track record**. Have there been incidents where MNOs or government are suspected or known to have engaged in surveillance, or to have used planned network outages as a tactic?

Remember the results from this exercise; you’ll be putting them to use in Sections 4.1 and 4.2, where participants assess risk and learn to plan with mobile (and related) security in mind.

**3. Instruction/Discussion (10 minutes):** Do you trust your technology providers?

If you haven’t done Section 3.1, Separation of Phone and State, have a short discussion here about the role of technology providers.

Technology providers include:

* Mobile Network Operators (MNOs).
* Providers of online services such as social networking, media hosting, and web-based email.
* Internet Service Providers (ISPs). Remember that ISPs can provide services direct to consumers, or they can provide services to other providers, for example by hosting websites that provide online services.
* Software providers. Have you ever read a EULA (end user license agreement)?

What is the relationship between technology providers and country governments (think especially about who allows or grants providers an operating license)? What about the governments in the country where providers are based? Do you trust some technology providers over others?

**4. Exercise (30 minutes):** Assessing operational security risks.

Work through the three areas given above to map out the operational environment for activists working on a particular issue, in a particular country. Use the [worksheet](https://docs.google.com/document/d/1MAb1DXYL6IYC-zNZsBtVKBPOuHhbVLfdze6kn7qxdnA/edit?hl=en_US) or a table with the same format projected on a screen or drawn on a board or whiteboard.

* For each area, ask what this means for mobile communications. Can communications be intercepted legally? Do you think communications are intercepted or filtered illegally or without your knowledge?

Options:

* Work through the exercise for participants’ own environment, or use a made-up scenario, either one that you write, or one from the [Guide to Mobile Security Risk Assessment](http://www.mobileactive.org/risk-assessment).
* Split participants up into groups according to country or sector of work and operation. Discuss, then report back (when you have a diverse or large group), or lead entire group through exercise from front of classroom.

**5. Risk Assessment Preparation Worksheet:** Operational Environment.

Every participant or group of participants who will be developing a risk assessment should complete their own copy of this [worksheet](https://docs.google.com/document/d/1MAb1DXYL6IYC-zNZsBtVKBPOuHhbVLfdze6kn7qxdnA/edit?hl=en_US) as preparation, detailing the operational environment in which they operate. This can be done during this section or as homework.