**Exercise 3: Code-making**

**Intro:** Hands-on exercise to teach participants how to create a functional code for communicating (both spoken and written communication) within the context of a given scenario.

**Timing:** 1.5 hours

**Equipment Needed:**

* 2 mobile phones per team.
* Paper to write down scenarios and/or pre-prepared scenarios.

**Content Outline and Main topics:**

1. **Discussion (15 minutes)**: How vulnerable to interception and spoofing are voice and SMS communication?
2. **Exercise/Instruction (45 minutes-1 hour)**: Code-making.
3. **Discussion (15-30 minutes)**: Report back.

**Objectives/Expected Outcomes:**

Participants will learn how to protect their tactical plans using simple codes.

**Content**

**1. Discussion (15 minutes)**: How vulnerable to interception and spoofing are voice and SMS communication?

Review with participants.

* What kind of content is sensitive?
  + Content sensitivity in coordination and communication.
    - Coordination details.
    - Content about event.
    - Names of those involved.
  + Evidence and documentation.
    - Documentation of illegal or incriminating activities.
    - Evidence that an adversary may want to tamper with or destroy.
* In what ways can voice calls be vulnerable?
  + Eavesdropping: in person or at the device-level or operator level
  + Known time, sender, recipient, cell tower location
* In what ways are SMSes vulnerable?
  + When they are sent in plain text. The text can be read, intercepted, and stored by the MNO.
  + Known sender, recipient, times, cell tower-location.
  + Can easily be stored centrally, logged, filtered for keywords, and made actionable for authorities quickly.
* If you have to use voice or text messaging, be as anonymous as possible.
  + Unregistered SIMs.
  + Unregistered handsets.
  + Location: always avoid calling or texting from home or work.
* Develop a code that fits your situation, be it a campaign, group, or organization
  + What is a code? Any way of getting your message across that disguises the true content.
  + Your code is only useful if it's easy to remember and use. You shouldn't need to write it down.

**2. Exercise/Instruction (45 minutes-1 hour)**: Code-making.

Divide participants into an even number of small groups. Give each set of two groups a scenario, and have them develop a code. They can write it down if they want to, but encourage them to try and memorize it.

Separate groups and have them participate in the action/event, communicating using their code. This can be done simultaneously by as many groups as you have trainers, or all together with some participants watching as each set of two groups try to communicate in code.

Use the events below to point out the importance of a code being used as part of a policy that builds in contingency plans.

* Give them new information and see how well their code works.
* Build in security issues: someone loses a phone, someone’s phone is broken, the mobile network is shut down, and so on. See if their code can withstand the given adverse event.

**Discussion**: Report back

* Ask each group to describe:
  + the scenario
  + one team member writes an SMS that incorporates new information
  + the SMS is read aloud in front of the whole group
  + the larger group has an opportunity to guess what the message means
  + after a few guesses, another team member who was not involved in drafting the SMS says what they think it means, discuss what changed, what they thought was happening
  + if the code doesn’t work, walk through the misunderstanding and extract issue areas

**3. Discussion (15-30 minutes)**: Report back.

Making flexible codes and planning for good, bad, and unexpected events.

Create a list of best practices for code-making based on exercise.

Things to highlight:

* Flexibility in code.
* Anticipate likely changes.
* Create code names for all key participants.
* Codes for things going wrong
* What are the limitations of using a code?
  + What if your code is broken? How will the other party know, or how will you communicate this to them?
  + Codes don’t work if infrastructure (the mobile network, for example) is shut down.
  + Always have a backup plan, such as a physical place to meet in person, or an alternative method of communicating when the network is down or you suspect you need to increase your security levels.
    - Consider apps for encrypted email, encrypted SMS, encrypted chat, or VOIP. This can be a PC app, too.