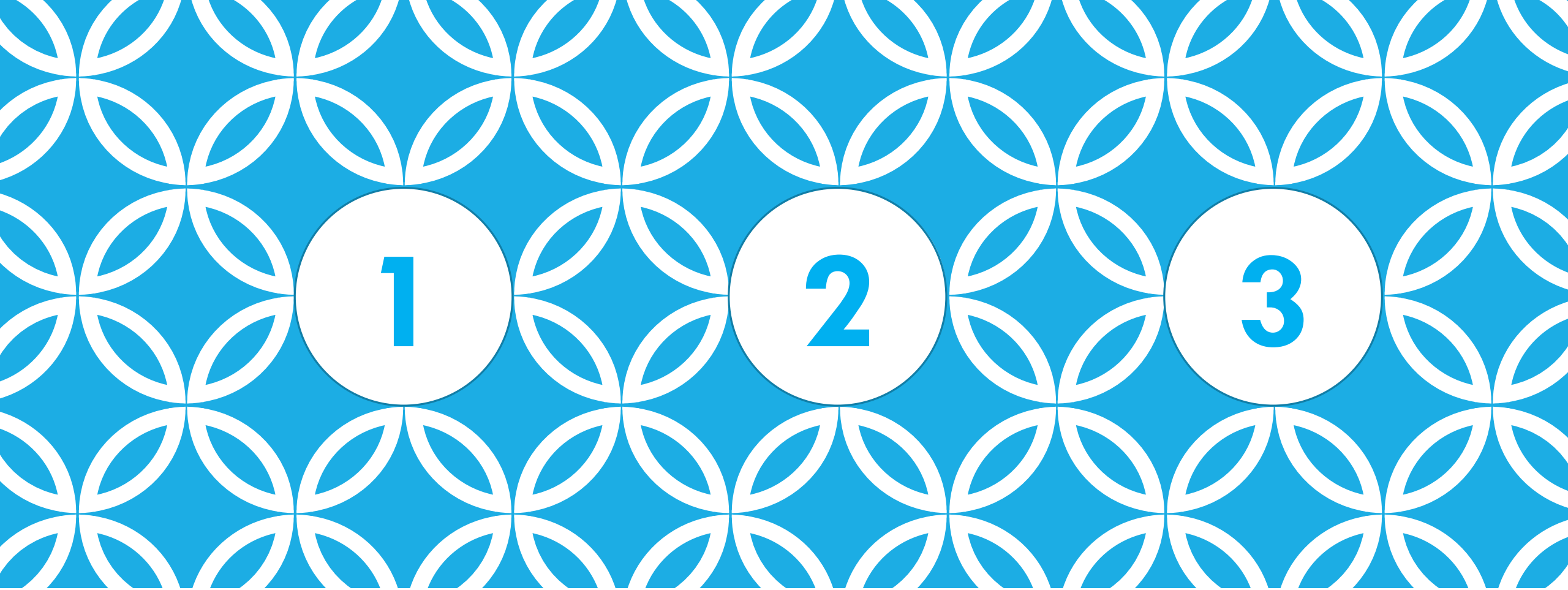


WI-FI ADAPTER, FINDER OR … JAMMER

1-2-3 with Globeron

Globeron

25 Sep 2017

DISCLAIMER – WIRELESS POLICY REGULATION

ITU (International Telecommunication Union)

Memorandum of Understanding (MoU) 2013 between IMPACT and Globeron Pte Ltd

International Multilateral Partnership Against Cyber Threats (IMPACT)

http://www.impact-alliance.org/download/pdf/media/whats-new/2013/IMPACT-Globeron-Release.pdf

Video: Wireless Cyber Security Risks – Practices for policy makers and regulators

https://www.youtube.com/watch?v=3DYp4g5R6lU

IMPORTANT - FCC REGULATION – JAMMERS

SIMILAR REGULATIONS APPLY FOR OTHER COUNTRIES

Enforcement Bureau

GPS, Wi-Fi, and Cell Phone Jammers
Frequently Asked Questions (FAQs)

https://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf

https://www.fcc.gov/general/jammer-enforcement

27 Jan 2015 - FCC Public Notice - WARNING: Wi-Fi Blocking is Prohibited

https://apps.fcc.gov/edocs_public/attachmatch/DA-15-113A1_Rcd.pdf

https://www.fcc.gov/document/warning-wi-fi-blocking-prohibited

SIGNAL GENERATORS.
2.4 GHZ AND 5 GHZ IS OFTEN CALLED THE "WI-FI" SPECTRUM

Exercise 1: try to find the "Wi-Fi" bands in the Spectrum Allocation Chart

https://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf

Answer: these **unlicensed** bands are called the **"Amateur"** bands

Many technologies are used in 2.4 GHz intentionally or unintentionally:

Wi-Fi, Bluetooth, Motion Detectors (Passive Infrared Devices – PIR), Baby Video Monitors, Video Transmitters, Microwave Ovens

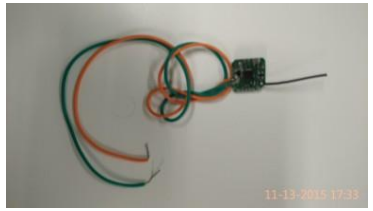
and in 5 GHz as well: Wi-Fi, LTE, Motion Detectors, Radars

Wi-Fi is the most popular and successful technology implemented in these Spectrum ranges

SIGNAL GENERATORS

All kind of intentional Signal Generators “Jammers”

Embedded



Single Board Computer with software written Linux Script to control the Wi-Fi Chips or Software Defined Radios

Wi-Fi Chips

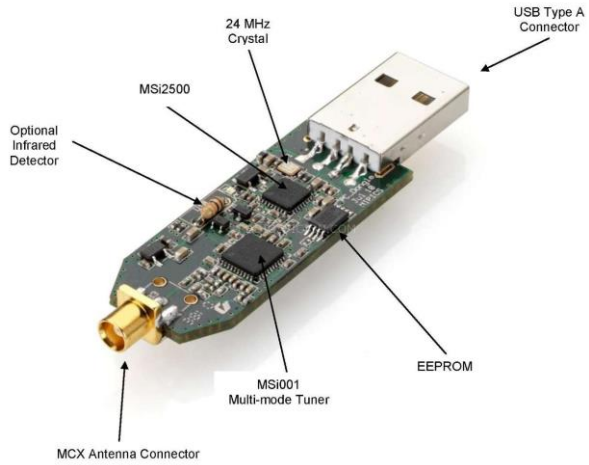
SDR

Wi-Fi vendors use APs with linux to test AP channel switching when there is RF interference (RRM,ARM,SmartRF,ChannelFly)

SIGNAL GENERATORS

Wi-Fi USB adapters “Dongles” or Software Defined Radios (SDR)

Millions of these devices are all approved by the government regulators and have a **FCC ID**



CLAUSE 6

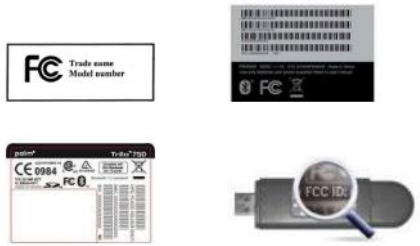
https://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf

6. Some devices claim to block cell phone calls, text messages, and emails only inside a car. Are these illegal as well?

Any device that jams or disrupts cell phone calls, text messages, or other wireless communications by emitting an interfering radio frequency signal is illegal and may not be marketed or operated in the United States, except in the very limited context of authorized, official use by the federal government. Please note that it may be difficult to determine from an advertisement how a particular device functions. You should contact the FCC's Enforcement Bureau at jammerinfo@fcc.gov if you have questions.

We emphasize that consumers *cannot* legally operate any radio transmitting device (e.g., a Wi-Fi or Bluetooth transmitter, wireless phone, etc.) that does not have an authorization from the FCC and that is not properly labeled with an FCC identification number. (See Figure 1 below.)

Figure 1: Sample FCC ID labels



Jamming devices, however, are *ineligible* to receive a grant of equipment authorization from the FCC or an FCC ID. (The FCC's Office of Engineering and Technology oversees the authorization of non-jamming equipment that uses the radio frequency spectrum. More information is available at http://www.fcc.gov/encyclopedia/equipment-authorization.)

We emphasize that consumers *cannot* legally operate any radio transmitting device (e.g., a Wi-Fi or Bluetooth transmitter, wireless phone, etc.) that does not have an authorization from the FCC and that is not properly labeled with an FCC identification number. (See Figure 1 below.)

Figure 1: Sample FCC ID labels

USB ADAPTER - EXAMPLE

Battery powered USB adapter with display

- No need to plug the device into a laptop to scan Wi-Fi networks in 2.4 GHz and 5 GHz it shows the SSIDs on the display (this is before the Smartphones became popular)
- or use it as a normal USB-Wi-Fi Adapter 802.11a/b/g in Windows/Linux/Apple OS
- It is FCC approved: ID S15WUB410
  - Approval - https://fccid.io/SI5WUB410
  - Inside photo (on the FCC website) - https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=557506\

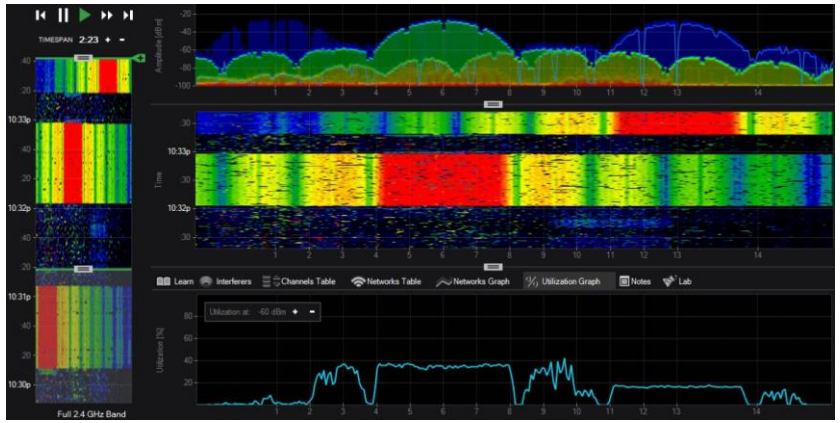
USB + WINDOWS SOFTWARE = SIGNAL GENERATION

FCC approved:
ID S15WUB410

+

=

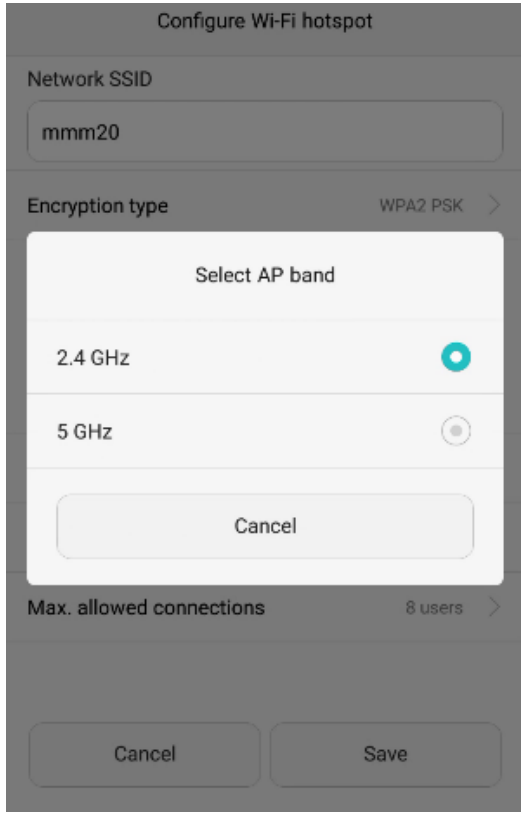
Channel 6 Channel 13

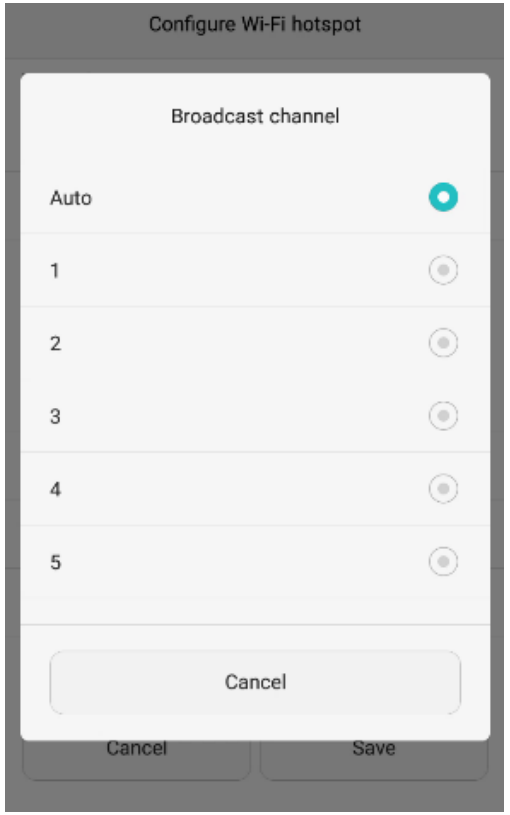


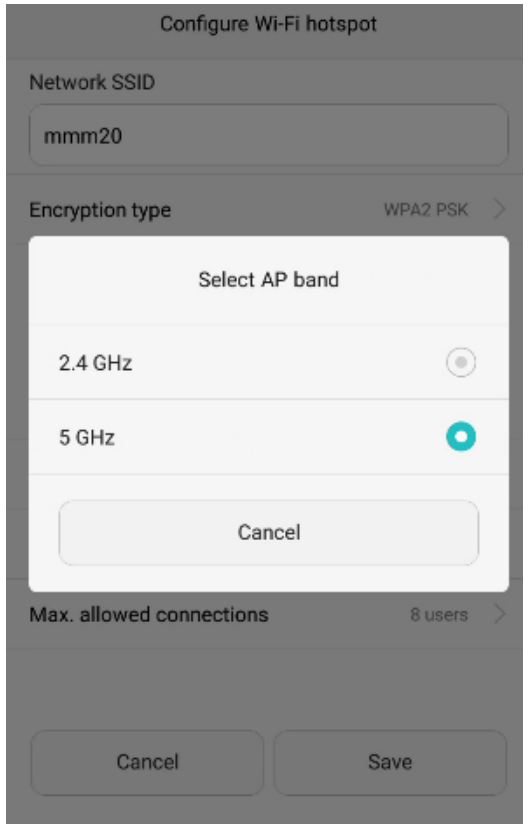
Or see it in action demo 3:
https://www.youtube.com/watch?time_continue=3496&v=VzFmNVAB3a8

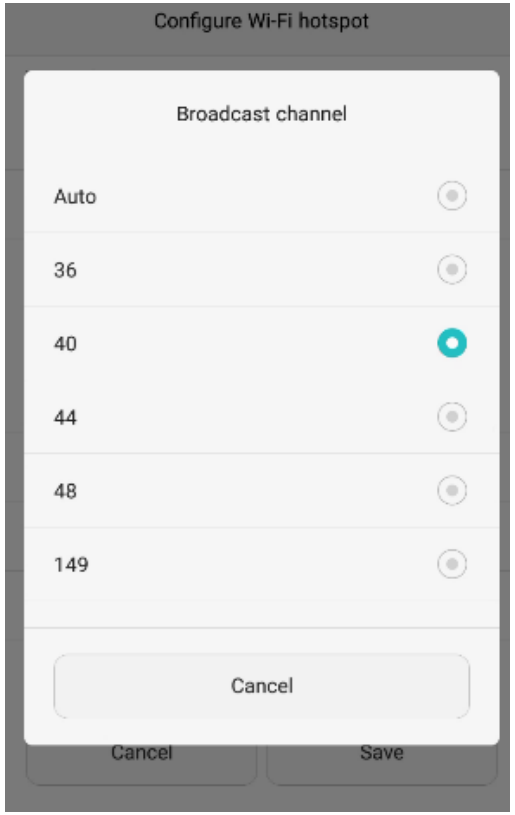
SMARTPHONES/TABLETS – WI-FI HOTSPOT / TETHERING

Most smartphones/tablets cannot configure the frequencies or channels and often create Adjacent Channel Interference (e.g. they transmit on channels like 2, 7, etc. in the 2.4 GHz frequencies impacting transmissions of APs on channel 1,6,11 Here is an Android smartphone that is flexible in the configuration, once configured the BSSID is random and therefore difficult to contain (e.g. to Deauthenticate)



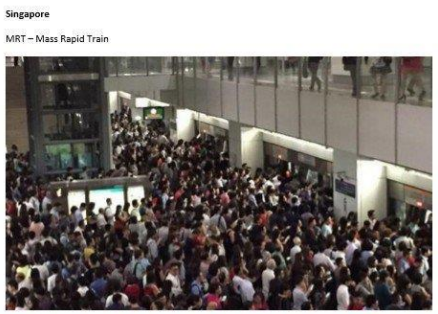






PUBLIC WI-FI NETWORKS AND MANY SMARTPHONES

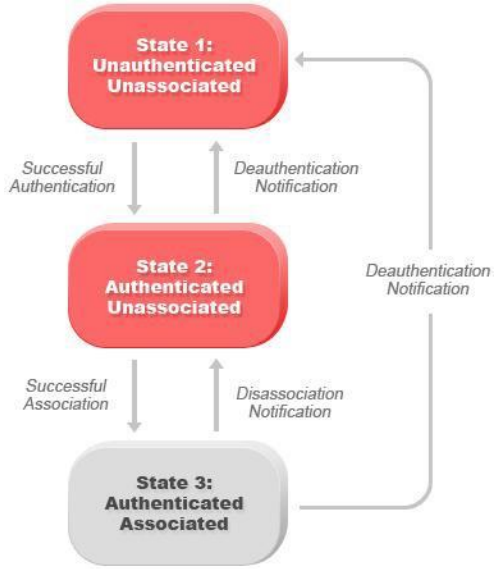
But what if everybody turns-on their Wi-Fi Hotspot on their smartphone at the same time at (Large) Public Venues, Concerts, Hotels, Schools, government/telco provided Wi-Fi networks in both 2.4 GHz / 5 GHz? What if everybody configures the same SSID (Service Set Identifier) e.g. “HotelPublicWiFi” ?



e.g. Tourists/ Families buy a local Sim-card and share the Wi-Fi with their family members

“JAMMERS” USING THE WI-FI PROTOCOL (OSI LAYER 2) “DE-AUTHENTICATION” / AIR-TERMINATION

Normal Wi-Fi operation (e.g. client disconnects or APs time-out on Auth.)

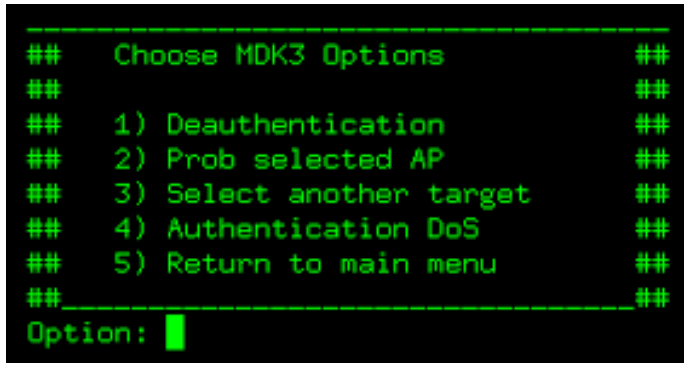


Intentional De-Authentication

Typically Linux scripts in tools

Kali Linux, Cyborg, etc.

and protocol analyzers doing “De-auth” packet injection



Wireless Intrusion Prevention Systems

Enterprise level systems using the

AP or AP/Sensor or Sensor only

to contain “Rogue” APs & Clients

CONCLUSION

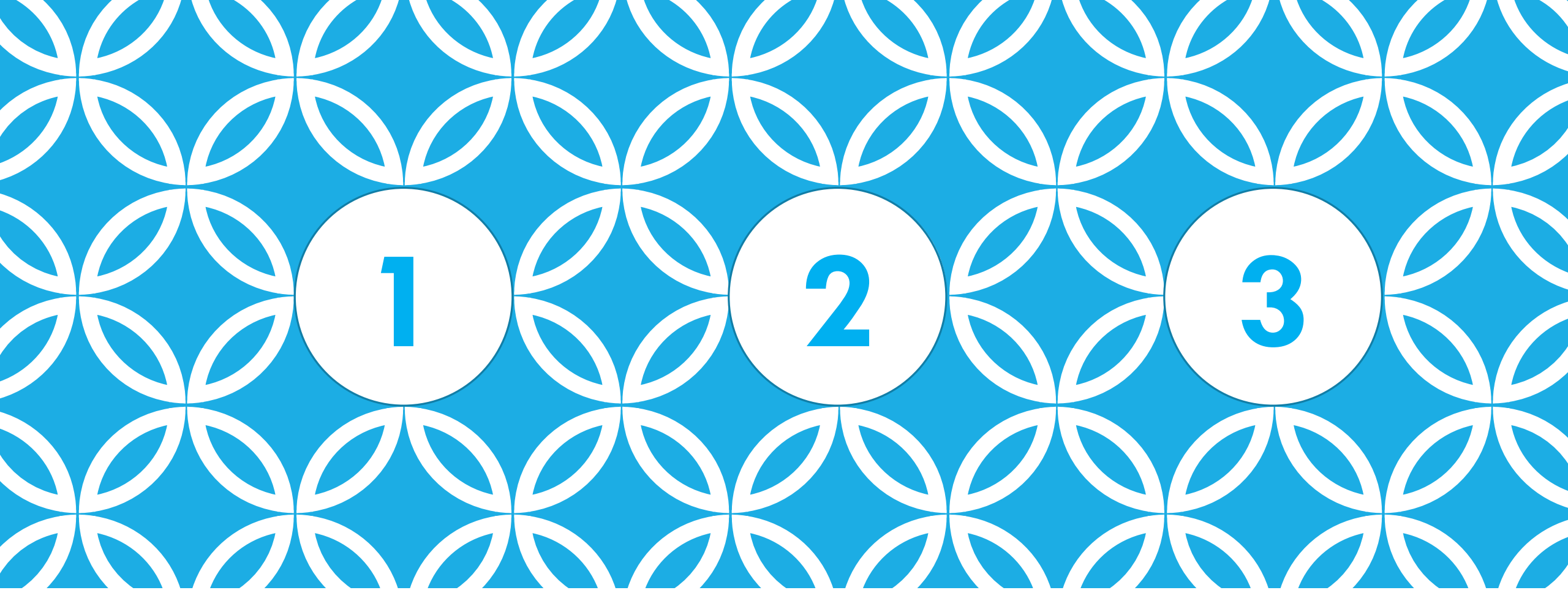
Policies and regulations maybe need to be adjusted for approved equipment by the government regulators ("FCC ID") as well how software may or may not be programmed or configured.

Is it possible to set regulations for unlicensed spectrum? (similar as licensed spectrum it is not mandated what type of technology can be used in the spectrum).

Wi-Fi tools and software need to be classified (e.g. Linux scripts, protocol analyzers)

Definitions need to be improved maybe per OSI-Layer (Physical, Data-Link, Application)

- Jamming and "RF-Jamming"
- Interference (Intentional / Unintentional)
  - Co-Channel and Adjacent Channel Interference
- Deauthentication ("DEAUTH") (normal operation and tweaked operations by "hackers")
- Disassociation
- Rogue AP, Rogue Client
  (e.g. what if someone configures his smartphone with the SSID of the organization")
- Wireless Intrusion Detection System (WIDS) and Wireless Intrusion Prevention System (WIPS)
  Air termination, Containment (Wi-Fi Isolation of clients, but that is AP related)



WI-FI ADAPTER, FINDER OR … JAMMER

1-2-3 with Globeron

Globeron