Intercepting Russian Military comms

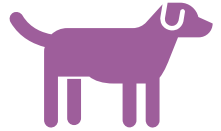
SIGINT for the people

./whoami

Go by DE7AULT online

2nd year cybersecurity student @ BU

I hack stuff



I like trolling Russian Military and Security services

SIGINT ?

- AKA "Signals Intelligence"
- Anything where signals are being intercepted
- Includes COMINT (Communication Intelligence)
- Includes ELINT (Electronic Intelligence)

The Three Problems

- What lead to Russias opsec failures?
- Underequipped
- Old tech
- Using captured equipment

The equipment problem

- Russian Army is massively underequipped (Equipment is often cold war era)
- Fake equipment being issued (Plastic body armour, plastic helmets)
- Using a lot of non-digital / Analogue communications
- Radio equipment is often not encrypted
- Local forces often forced to communicate through messaging apps on both their own and captured Ukrainian phones as they can't securely reach HQ

The tech problem

Captured Russian Equipment has shown a lot of current forces are using civilian, Chinese-made Baofeng radios (UV-5R and UV-82)

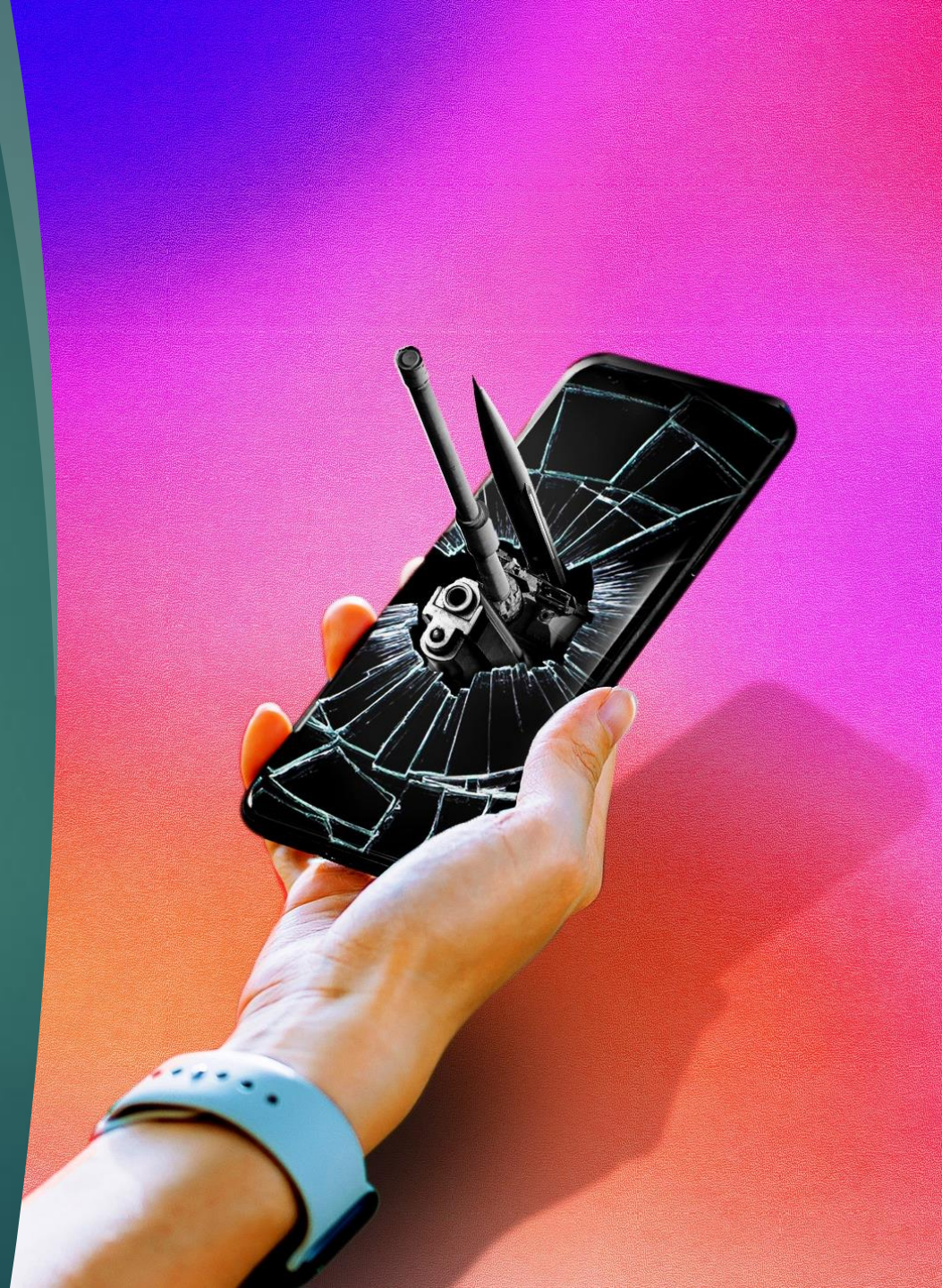
Even their long-range military radios are Soviet Era and completely analogue with no encryption

Russian forces have resorted to using one-time pads for important communication, the old-school cipher itself is secure, but the key exchange is not.

> Almost no one can get a hold of central command, it's not even a matter of jamming, there's just no long range commo quipment or relays that went with the troops there.

The phone problem

- Lack of mil-spec communications equipment leads to Russian forces using their phones
- Ukrainian cell providers block Russian cellular usage
- Russian forces take Ukranian phones
- Ukrainian cell providers start using the captured phones as listening devices
- Lose – Lose situation for Russian forces

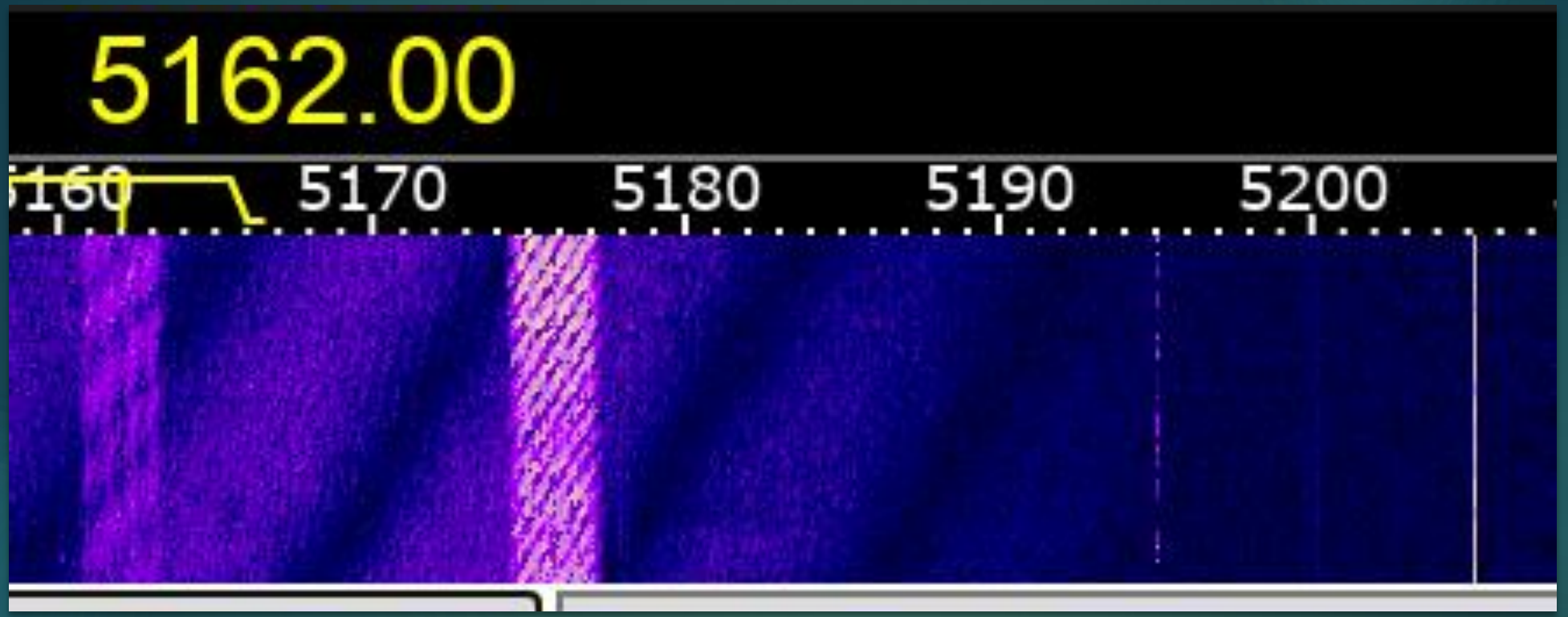


Slight issue

This level of snooping isn't really accessible to us

Unless someone in this room works with Ukrainian Intelligence

So what can we do?



Intercepting radio at home

sign	Note				
EA4	Air Force HQ Moscow	8.162	CW		Russian Strategic Air Force Bombers T-95 Ground Autumn Primary Frequency
EJX		8.170	CW	6PLS D2WD	Russian Strategic Air Force Bombers TU-95 Spring Air CW Frequency
EA4	Air Force HQ Moscow	8.816	CW		Naval Air Transport
a Radio	Sometimes call checks Il-76	8.847	USB		Traffic control comms air force Chkalvosky Moscow Region
Ja Skat 07	Possible Air Force use	8.895	CW		Russian Strategic Air Force TU-95 Summer CW Ground
	Russian Strategic Air Force TU-95 ground CW frequency				
	Russian Strategic Air Force CW Ground Frequency	8.909	USB	OCHI STKA, PROC ELKA	Russian Strategic Air Force Summer TU-95 Frequency
ARJ	72131, 72132-TU-22 from Renchovo				
	Russian Strategic Air Force TU-95 CW ground frequency	8.252	USB		
SELOK RSAR NETIST	Traffic control comms air force Chkalvosky Moscow Region	9.027	CW		
EA4	Air Force HQ Moscow	9.128	CW	P7YR W SY QYY	
	Russian Strategic Air Force Bombers TU-95 CW Ground Spring Primary Frequency	11.072	CW	RE A4	Air Force HQ Moscow
BOR PORA	Russian Strategic Air Force Bombers TU-95 Spring Frequency	11.354	USB	RJF94 / N OVATOR PRI BOJ KRO CKET	Russian Naval Air Transport Command
	Russian Strategic Air Force Bombers TU-95 Autumn Frequency	11.360	USB	PROSELOK KORSAR	Traffic control comms air force Chkalvosky airfield Moscow Region
KATOLIK	Russian Strategic Air Force TU-95 CW Winter ground frequency				
KATOLIK	Russian Strategic Air Force Bombers TU-95 Winter Frequency	18.030	USB	KORSAR	Traffic control comms air force Chkalvosky Moscow Region

Frequency	Callsign
3395.5	RCV
4079	RMP
4635	
4376.5	
5411	RCJ
5717	RCV
8120	RAA
8345	
8348	
11000	RIW
11155	RIT
12464	
14556	RIW
19201	RCV

Step 1: Find the channels

- Probably the hardest part
- Need a Russian speaker
- Channels rotate every couple of weeks – every couple of months (HQ channels remain longer)
- Look near previously known frequencies
- When they do rotate, they often aren't far from original frequency

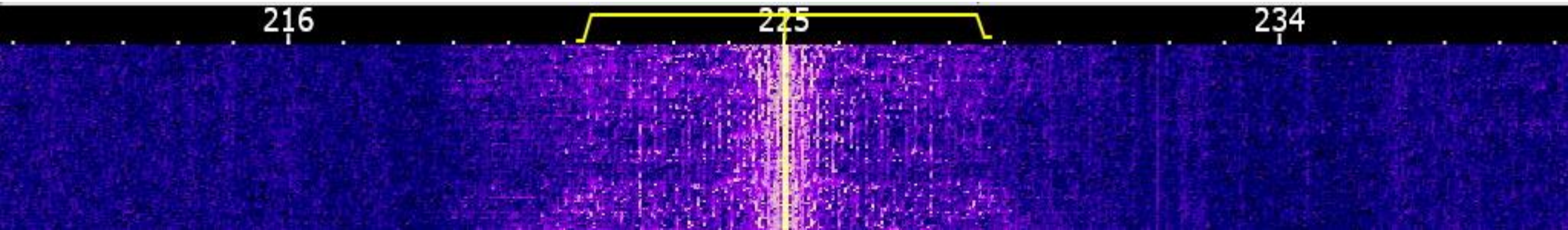
Step 2: Listen

You have two options:

A: travel to Ukraine and intercept russian radio communications directly
B: Use a webSDR (Web "Software Defined Radio")

Assuming the second option, the following webSDR has been effective for me (second is their experimental version)

http://websdr.ewi.utwente.nl:8901/
http://websdr.ewi.utwente.nl:8901/m.html/



Step 3: Discover Interesting Russian comms


It's really that
easy