Voice Cloning Air Traffic Control: Vulnerabilities at Runway Crossings

Andrew Logan

HelicoptersofDC@ProtonMail.com




Let’s rehearse that.

Who Am I

Andrew Logan

Professional Audio Engineer

Def Con 30 (2022): “Tracking the Military Ghost Helicopters of DC”



https://www.congress.gov/members/find-your-member

Say you support:

Safe Operation of Shared Airspace Act of 2025

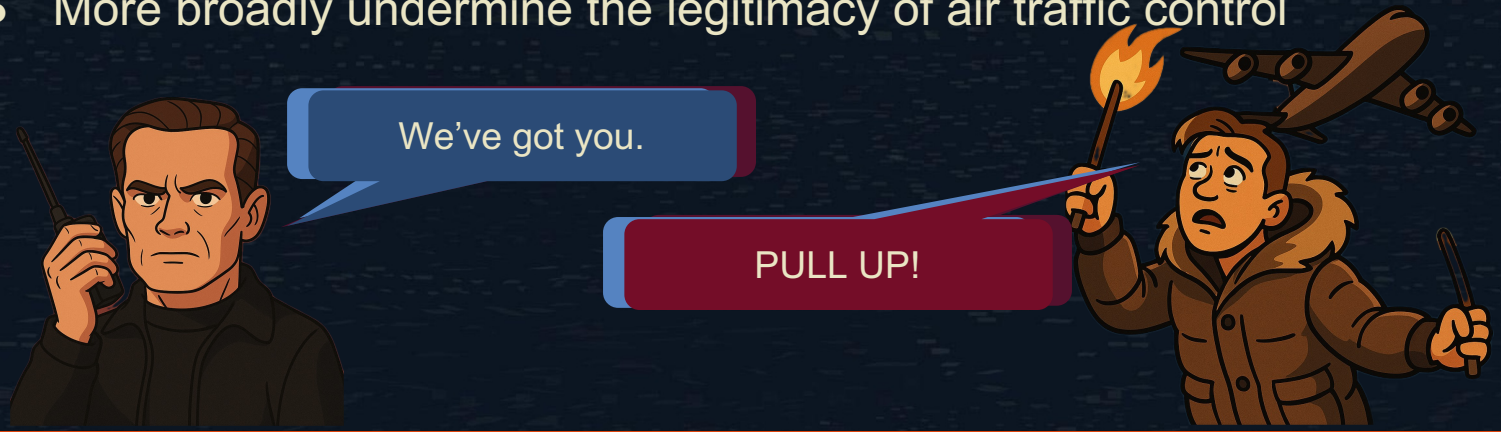
Bills that broaden the use of ADS-B

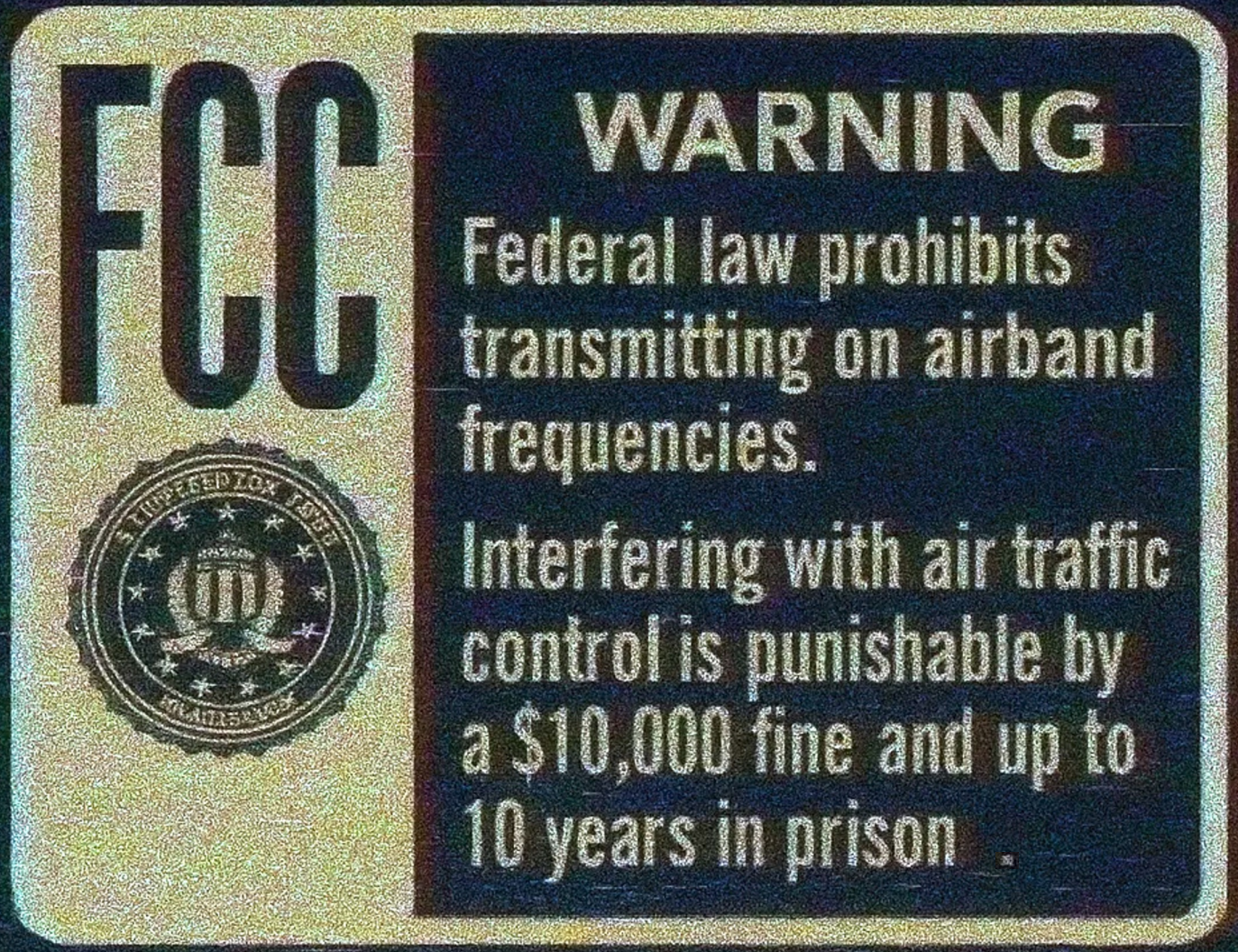


My Nightmare:

- A sophisticated attacker impersonating air traffic controllers
- Intermittently giving false clearances to cross runways
- In adverse weather conditions

- Could cause crashes
- More broadly undermine the legitimacy of air traffic control




FCC
WARNING
Federal law prohibits transmitting on airband frequencies.
Interfering with air traffic control is punishable by a $10,000 fine and up to 10 years in prison .

01 AM “Airband” Radio

01 AM “Airband” Radio

02 Voice Cloning Technologies

01 AM “Airband” Radio

02 Voice Cloning Technologies

03 Why runway crossings are most at risk

01 AM “Airband” Radio

02 Voice Cloning Technologies

03 Why runway crossings are most at risk

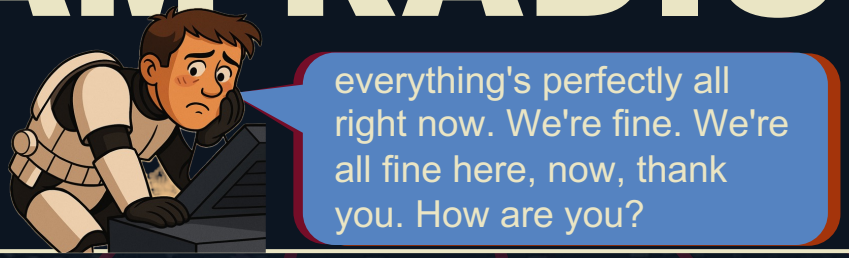
04 How to mitigate this threat

DISCLOSURES

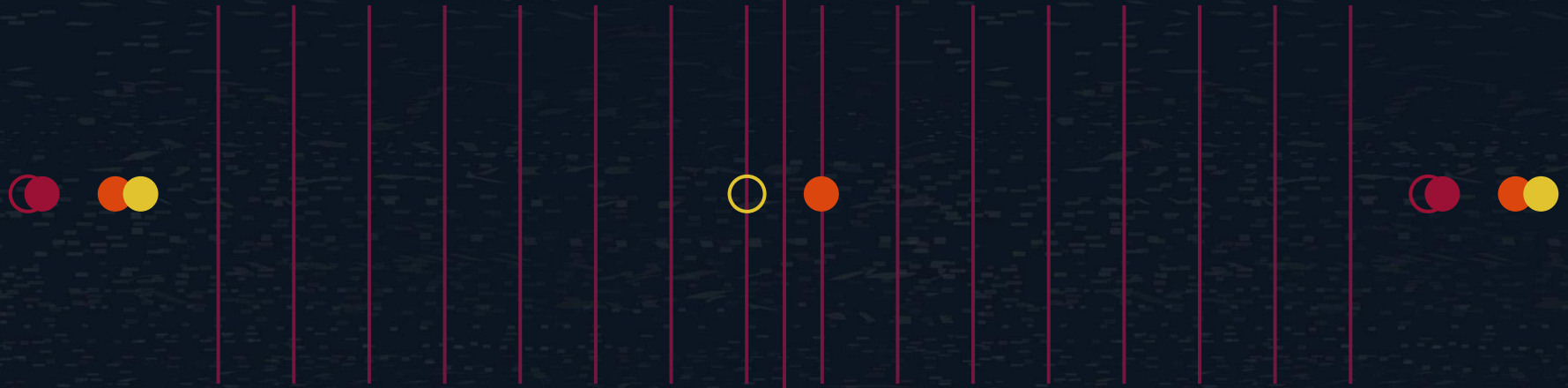
- **U.S. Senate Committee on Commerce, Science, & Transportation**
- **NATCA – National Air Traffic Controller Assoc.**
- ICAO – International Civil Aviation Organization
- CISA - Cybersecurity and Infrastructure Security Agency
- FAA – Federal Aviation Association
- FCC - Federal Communications Commission

PLAY

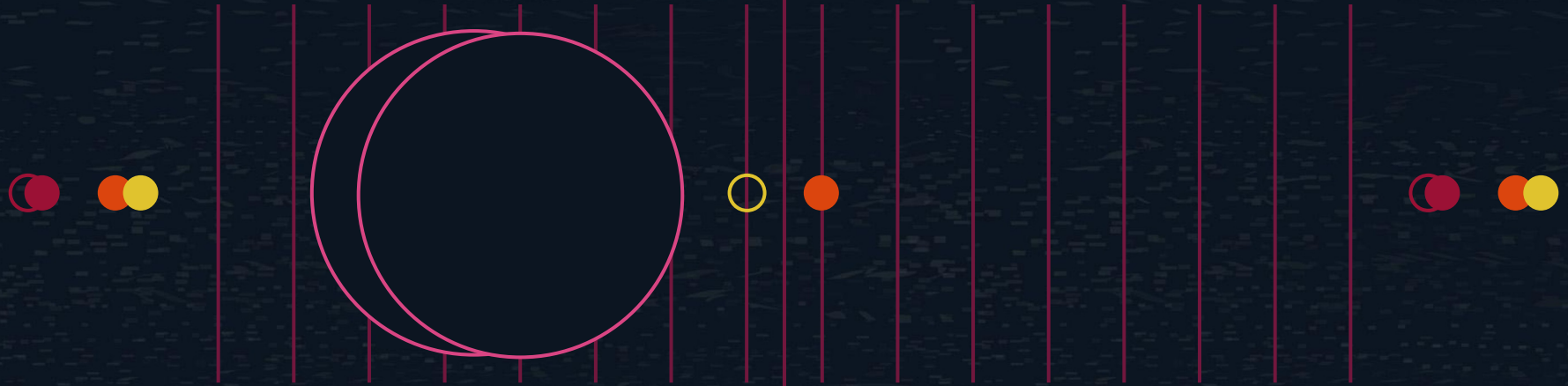
01
AM RADIO



AM RADIO CHARACTERISTICS

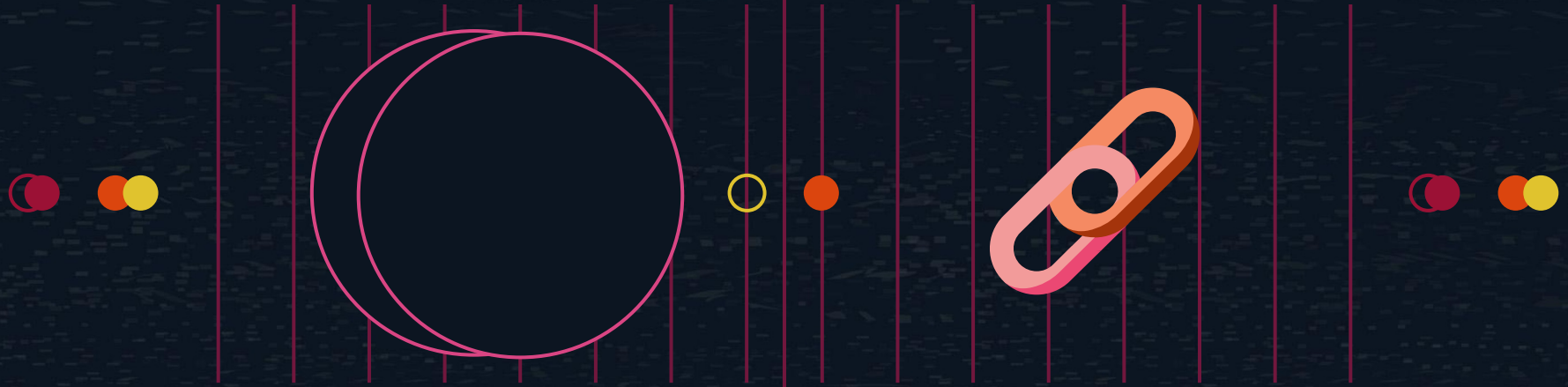


AM RADIO CHARACTERISTICS



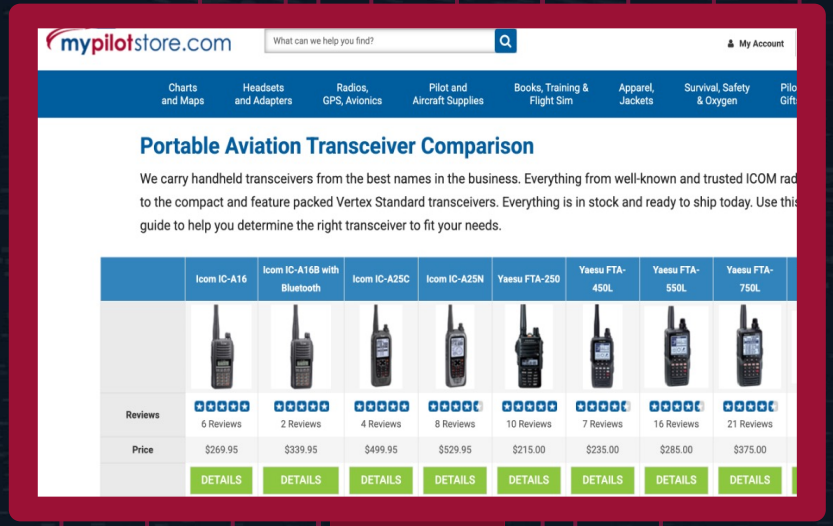
Allows for “heterodyning of carriers”

AM RADIO CHARACTERISTICS



Allows for “heterodyning of carriers”

Weak Capture effect compared to FM and digital modes



Commercially Available AM Transceivers



Motorola CM-400 VT VHF Transmitter Air Band Make Offer!

Shems Electric LTD (490)
100% positive · Seller's other items · Contact seller

US $400.00
or Best Offer

as low as $37.05/mo with Klarna. Learn more

Condition: **For parts or not working**

Buy It Now

Secondhand Tower Systems

- HF Radio (analog)

Digital and Other Modes

Digital and Other Modes

- HF Radio (analog)
- Aircraft Communications Addressing and Reporting System (ACARS)

Digital and Other Modes

- HF Radio (analog)
- Aircraft Communications Addressing and Reporting System (ACARS)
- VHF Data Link Mode 2 (VDL Mode 2)

Digital and Other Modes

- HF Radio (analog)
- Aircraft Communications Addressing and Reporting System (ACARS)
- VHF Data Link Mode 2 (VDL Mode 2)
- Controller-Pilot Data Link Communications (CPDLC)

Digital and Other Modes

- HF Radio (analog)
- Aircraft Communications Addressing and Reporting System (ACARS)
- VHF Data Link Mode 2 (VDL Mode 2)
- Controller-Pilot Data Link Communications (CPDLC)
- L-band Digital Aeronautical Communications System (LDACS)

Digital and Other Modes

- HF Radio (analog)
- Aircraft Communications Addressing and Reporting System (ACARS)
- VHF Data Link Mode 2 (VDL Mode 2)
- Controller-Pilot Data Link Communications (CPDLC)
- L-band Digital Aeronautical Communications System (LDACS)



Digital and Other Modes

- HF Radio (analog)
- Aircraft Communications Addressing and Reporting System (ACARS)
- VHF Data Link Mode 2 (VDL Mode 2)
- Controller-Pilot Data Link Communications (CPDLC)
- L-band Digital Aeronautical Communications System (LDACS)





Digital and Other Modes

- HF Radio (analog)
- Aircraft Communications Addressing and Reporting System (ACARS)
- VHF Data Link Mode 2 (VDL Mode 2)
- Controller-Pilot Data Link Communications (CPDLC)
- L-band Digital Aeronautical Communications System (LDACS)







Digital and Other Modes

- HF Radio (analog)
- Aircraft Communications Addressing and Reporting System (ACARS)
- VHF Data Link Mode 2 (VDL Mode 2)
- Controller-Pilot Data Link Communications (CPDLC)
- L-band Digital Aeronautical Communications System (LDACS)






Digital and Other Modes

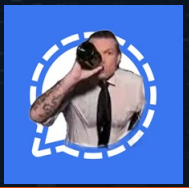
- HF Radio (analog)
- Aircraft Communications Addressing and Reporting System (ACARS)
- VHF Data Link Mode 2 (VDL Mode 2)
- Controller-Pilot Data Link Communications (CPDLC)
- L-band Digital Aeronautical Communications System (LDACS)











INTERPERSONAL ELEMENTS OF ATC

is it a single factor trust system?

01

Channel

Are you transmitting on the correct channel

INTERPERSONAL ELEMENTS OF ATC

is it a single factor trust system?

01

Channel

Are you transmitting on the correct channel

02

Voice

Do you sound authentic

INTERPERSONAL ELEMENTS OF ATC

is it a single factor trust system?

01

Channel

Are you transmitting on the correct channel

02

Voice

Do you sound authentic

03

Syntax & Validity

Is the command formatted and timed correctly

INTERPERSONAL ELEMENTS OF ATC

is it a single factor trust system?

01

Channel

Are you transmitting on the correct channel

02

Voice

Do you sound authentic

03

Syntax & Validity

Is the command formatted and timed correctly

04

Expectation

Is the command expected or a response to a prior request

FCC ENFORCEMENT TECH



Direction Finding Vehicles



Charles Cooper. Pirate Radio and FCC Enforcement

FCC ENFORCEMENT TECH



Direction Finding Vehicles



Fixed Direction Finding Stations



Charles Cooper. Pirate Radio and FCC Enforcement

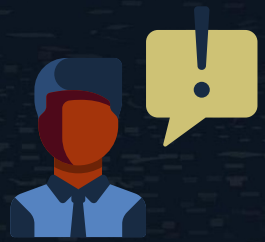
FCC ENFORCEMENT TECH



Direction Finding Vehicles



Fixed Direction Finding Stations

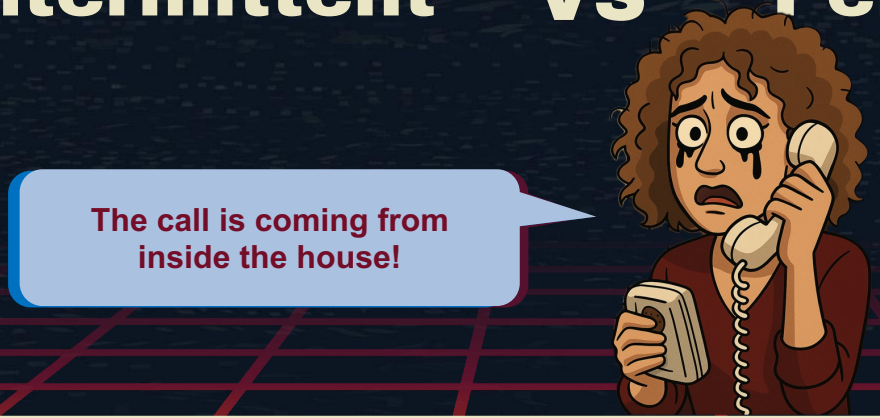


Field Investigative Agents



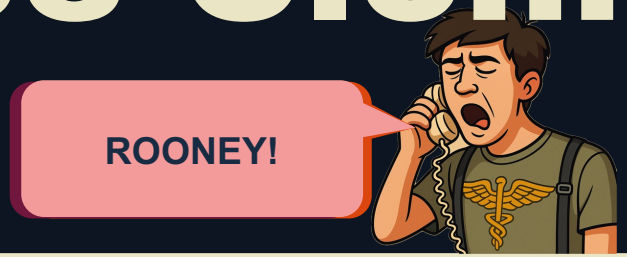
Charles Cooper. Pirate Radio and FCC Enforcement

Intermittent vs Persistent



PLAY

02
Voice Cloning



VOICE CLONING TECH

01

Voice Encoder

Captures Voice Characteristics

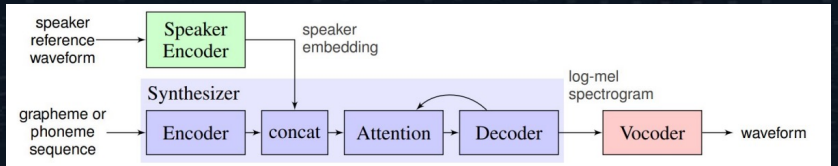


Figure 7: The SV2TTS framework during inference. The blue blocks represent a high-level view of the Tacotron architecture modified to allow conditioning on a voice. Figure extracted from (Jia et al., 2018).

Automatic Multispeaker Voice Cloning. Corentin Jemine. Master's thesis, Université de Liège, 2019.

VOICE CLONING TECH

01 **Voice Encoder**
Captures Voice Characteristics

02 **Text-to-spectrogram Synthesizer**
generates a spectrogram from text

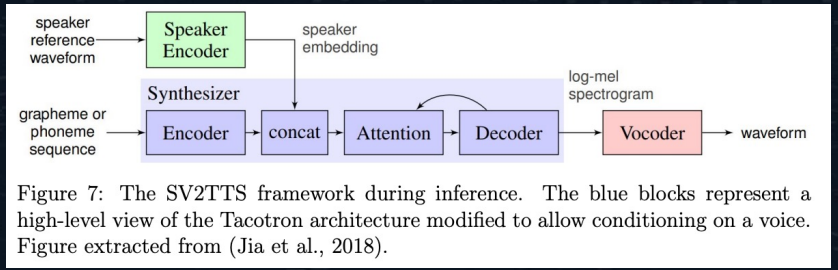


Figure 7: The SV2TTS framework during inference. The blue blocks represent a high-level view of the Tacotron architecture modified to allow conditioning on a voice. Figure extracted from (Jia et al., 2018).

Automatic Multispeaker Voice Cloning. Corentin Jemine. Master's thesis, Université de Liège, 2019.

VOICE CLONING TECH

01 **Voice Encoder**
Captures Voice Characteristics

02 **Text-to-spectrogram Synthesizer**
generates a spectrogram from text

03 **Vocoder**
infers an audio waveform from the spectrogram

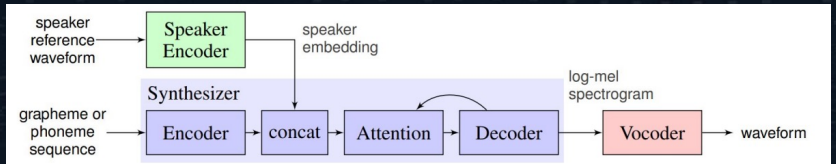


Figure 7: The SV2TTS framework during inference. The blue blocks represent a high-level view of the Tacotron architecture modified to allow conditioning on a voice. Figure extracted from (Jia et al., 2018).

Automatic Multispeaker Voice Cloning. Corentin Jemine. Master's thesis, Université de Liège, 2019.

Guardrails

Guardrails

- Verification before cloning celebrities/public figures

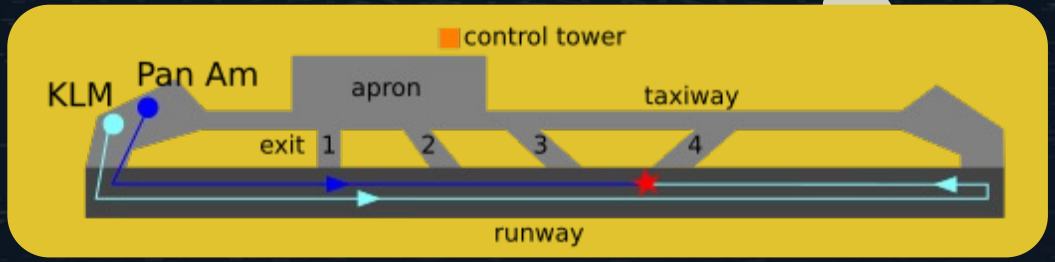
PLAY

03 RUNWAY CROSSINGS

Tenerife Disaster







Los Rodeos Airport, **Tenerife**, Canary Islands, Spain, March 27, 1977

583 fatalities: deadliest accident in aviation history.

Haneda Crash



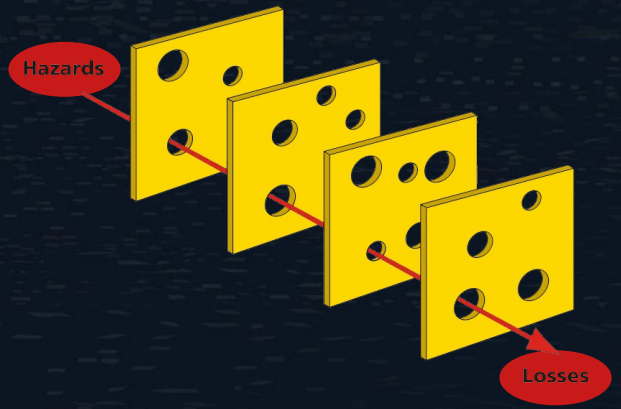


Haneda (Tokyo), Japan,
January 2, 2024

Japanese Coast Guard entered runway as Japan Airlines Flight 516 was landing

Haneda Crash







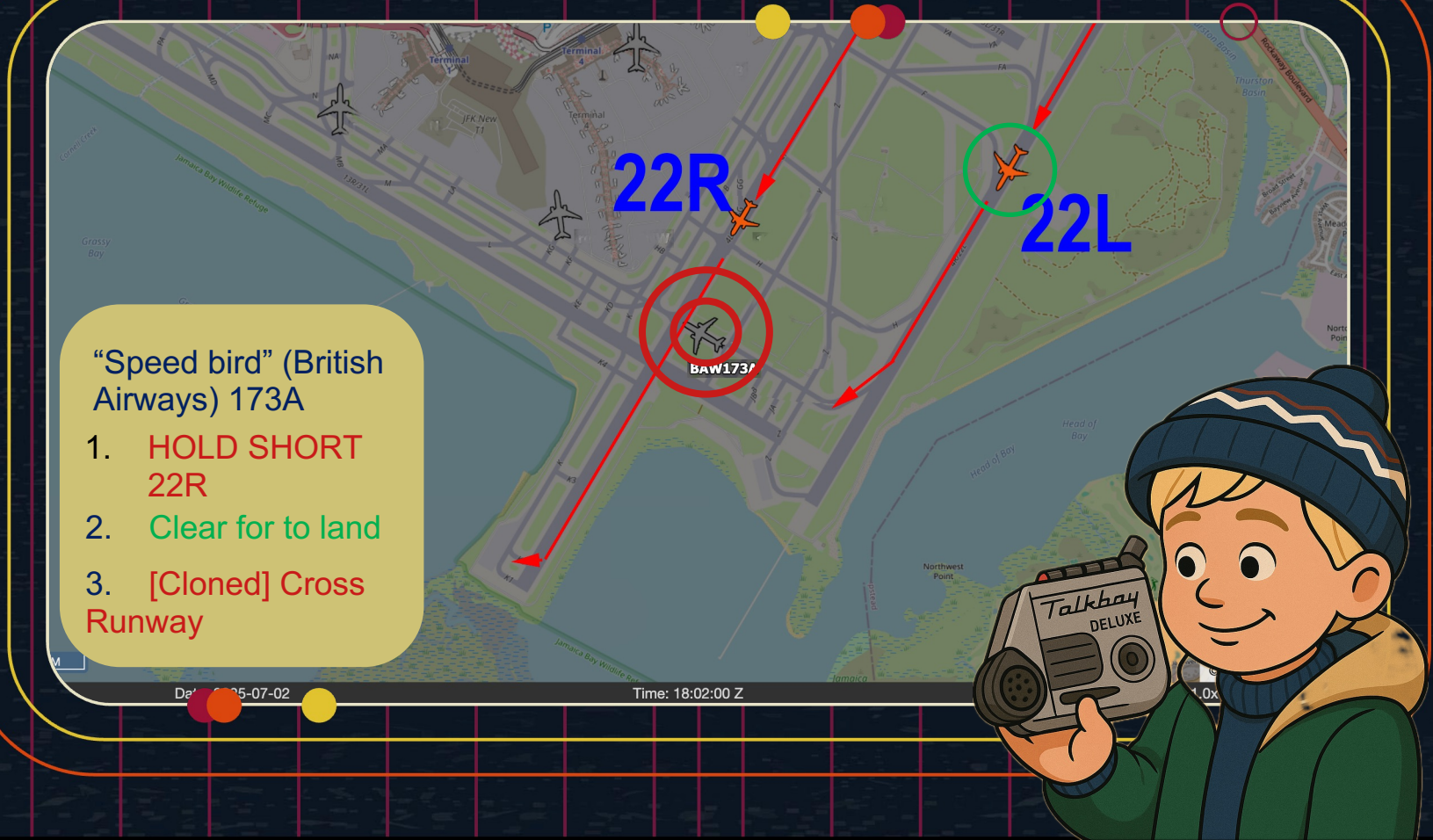
Haneda (Tokyo), Japan, January 2, 2024

Japanese Coast Guard entered runway as Japan Airlines Flight 516 was landing


22R
22L
BAW173A
“Speed bird” (British Airways) 173A
Time: 18:02:00 Z
Speed: 1.0x
© OpenStreetMap


22R
22L
BAW173A
"Speed bird" (British Airways) 173A
1. HOLD SHORT 22R
Time: 18:02:00 Z
Speed: 1.0x
© OpenStreetMap


22R
22L
BAW173A
"Speed bird" (British Airways) 173A
1. HOLD SHORT 22R
2. Clear for to land
Time: 18:02:00 Z
Speed: 1.0x
© OpenStreetMap


22R
22L
BAW173A
"Speed bird" (British Airways) 173A
1. HOLD SHORT 22R
2. Clear for to land
3. [Cloned] Cross Runway
Time: 18:02:00 Z
Talkboy
DELUXE

Additional Audio Examples

Additional Audio Examples



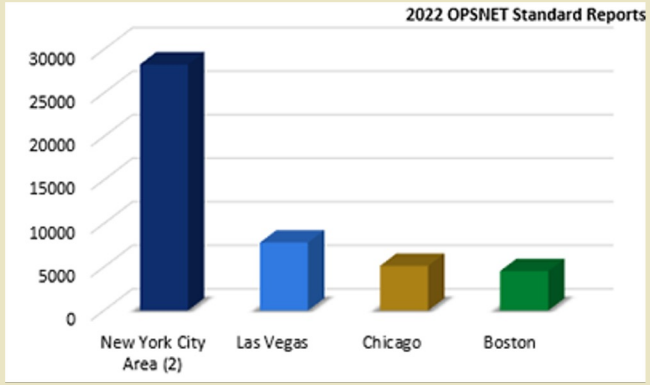
PLAY

04 MITIGATION



Make a move and the bunny gets it.

Threat Modeling



FAA Airports with most weather delays

STOP BARS

“If the stop bar lights have not been switched off after receipt of a clearance, the pilot or vehicle driver **must** seek clarification from ATC. Do not cross an illuminated stop bar."



Automation and Enhanced Vision in the cockpit

- Traffic Collision Avoidance System (TCAS)
- Enhanced Flight Vision Systems
  - Cameras
  - Infrared cameras
  - Radar

Sources via Google Sheet

Andrew Logan

X/Instagram/BlueSky: @HelicoptersofDC
Mastodon: HelicoptersofDC@DefCon.Social

HelicoptersofDC@ProtonMail.com

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**

Please keep this slide for attribution