CLICK AND DRAGGER

Denial and Deception on Android

- the grugq [@thegrugq]

AGENDA

- OPSEC Refresher
- Phones Suck
- Threat Model
- Some Solutions
- Conclusion

BUDA'S WAGON
A BRIEF HISTORY OF THE CAR BOMB
MIKE DAVIS
VERSO

Larry D. Benson Editor
Chaucer
The Canterbury Tales
HOUGHTON MIFFLIN

Orlov
Handbook of Intelligence and Guerrilla Warfare

URVEILLANCE TRADECRAFT
Peter Jenkins

Intelligence Tradecraft: Secrets of Spy Warfare
MK Dhar
MANAS

WITHOUT CLOAK OR DAGGER
BY MILES COPELAND
SIMON AND SCHUSTER

CONFIDENTIAL
Business Secrets
Getting Theirs -
Keeping Yours
JOHN NOLAN
Yardley Chambers

ABOUT ME

SAWYER
THE TAO OF SPYCRAFT
中國古諜史話
Westview

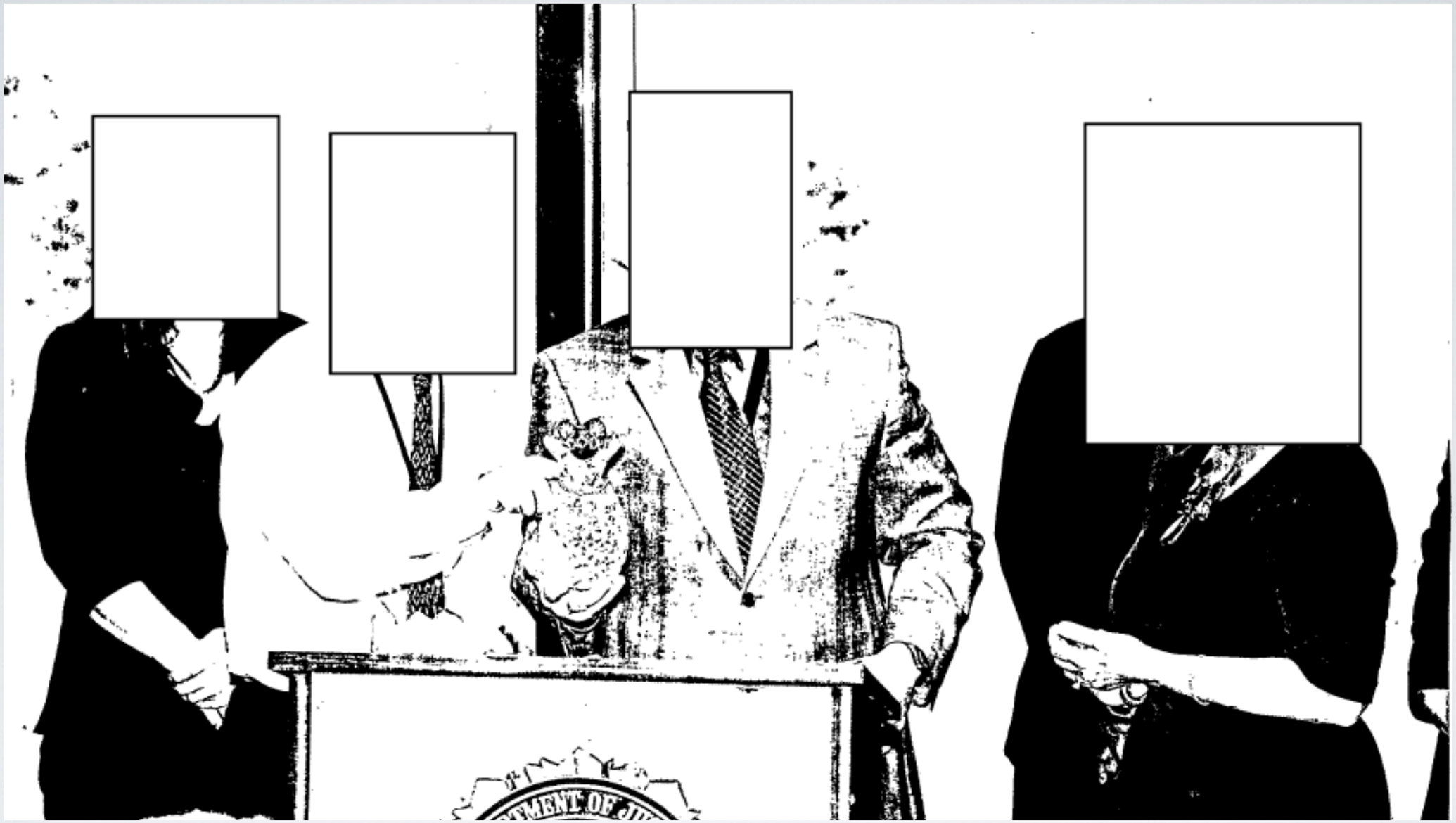
HOW TO LOOK FOR TROUBLE
A STRATFOR BOOK

CRIME PAYS
Making Your Living with a Life of Crime
KING

Edwin Hardin Sutherland
The Professional Thief
Chicago

CLANDESTINE OPERATIONS
PIERRE LORAIN
MACMILLAN

DUBEY | MISRA
ANDROID SECURITY
CRC



OPERATIONAL SECURITY

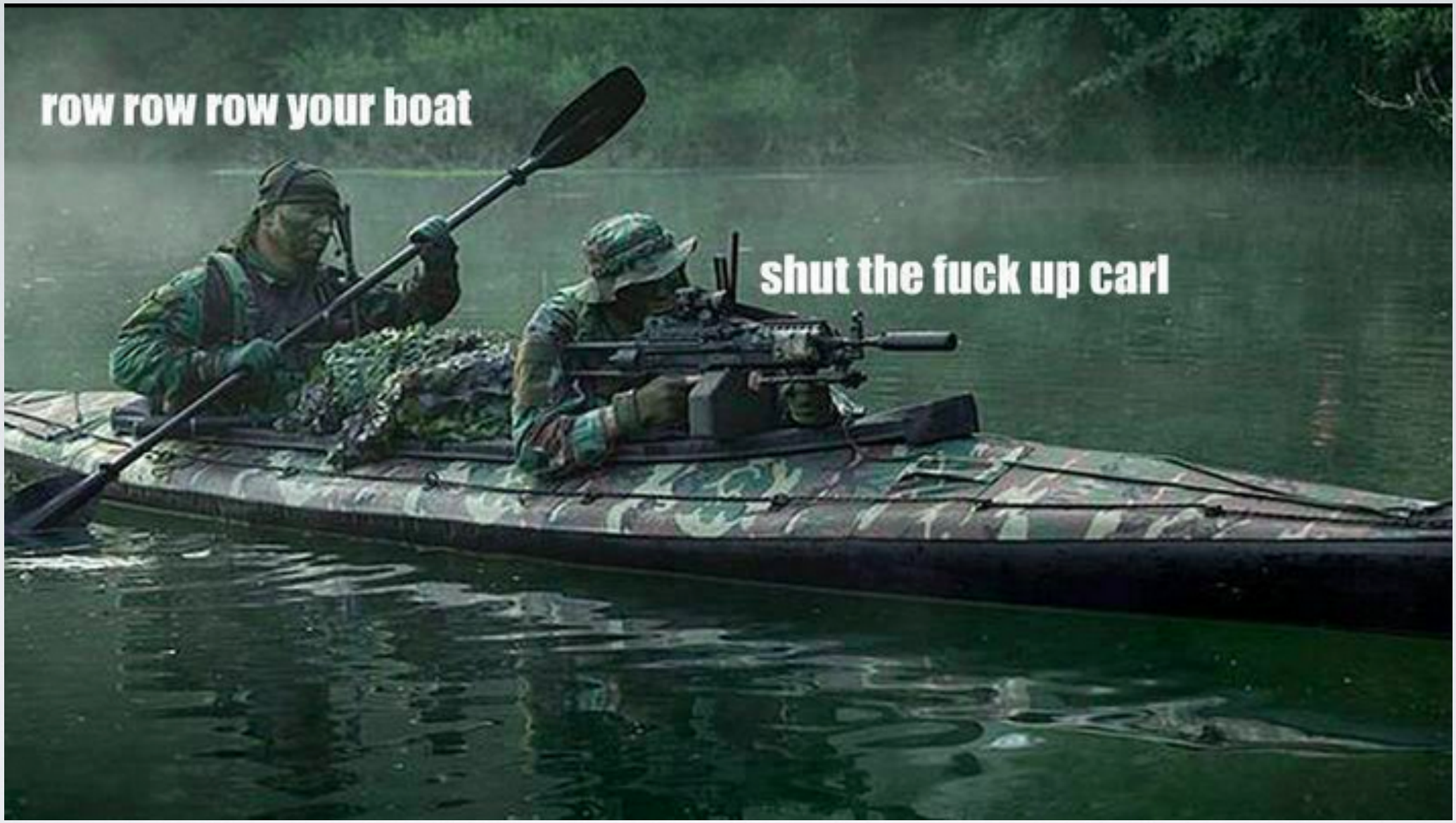
The Short Version


SHUT YOUR DAMN
PIE HOLE!
JOHNSTON
U.S. ARMY
Think OPSEC
US
INF

"If you want to lose a fight, talk about it first"

–Quellcrist Falconer

DENIAL & DECEPTION



DENIAL

Prevent the adversary from gaining useful information

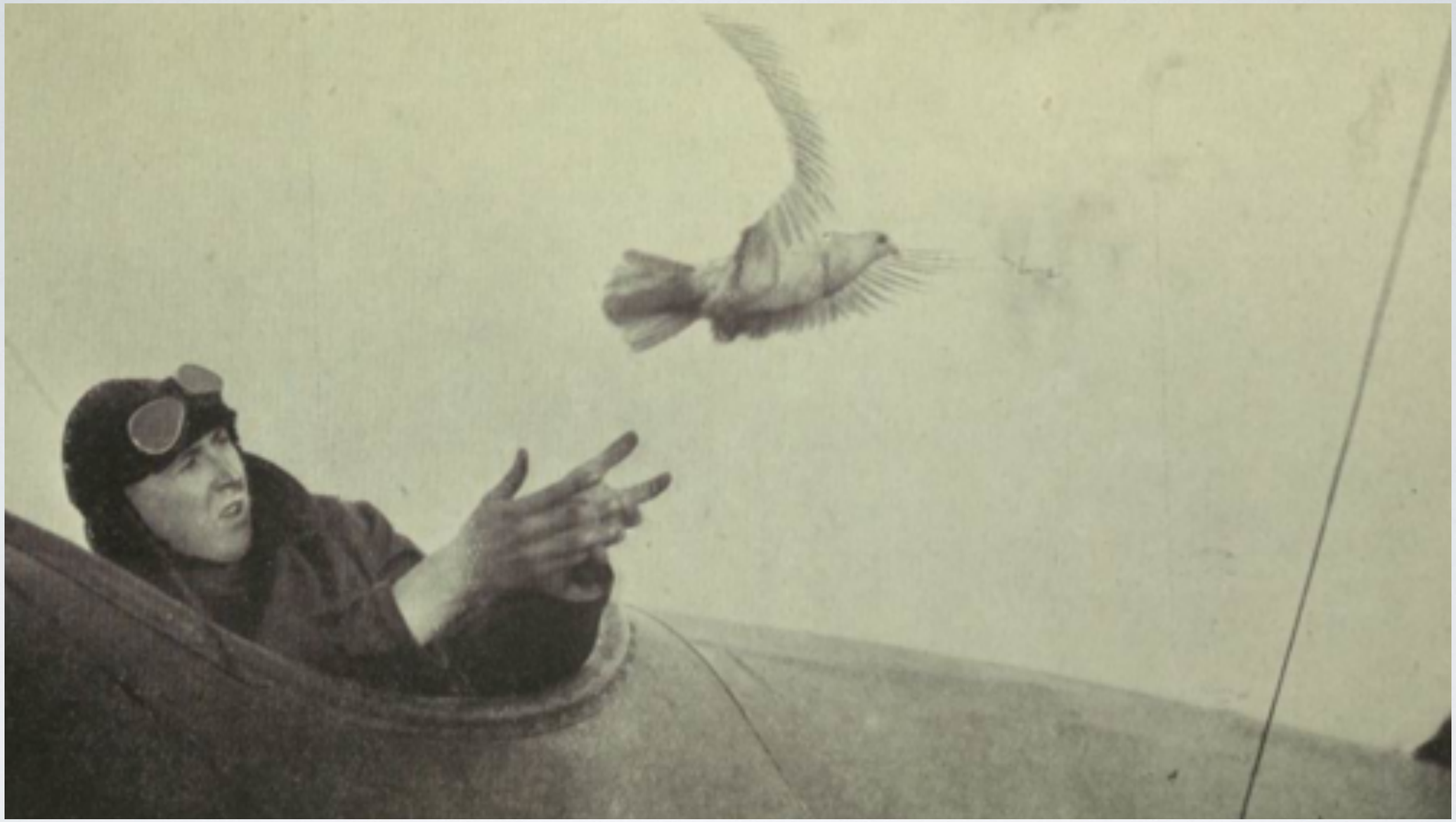
DECEPTION

Feed the adversary false information

- Cover
  - Cover for action
  - Cover for status
- Concealment
- Compartmentation

"People must communicate. They will make mistakes and we will exploit them."

–James Clapper, Director of National Intelligence



PHONES SUCK

"The greatest material curse to the profession, despite all its advantages, is undoubtedly the telephone."

–Allen Dulles,
Former Director of Central Intelligence

NO MOBILE ANONYMITY

MOBILE IDENTIFIERS

LOCATION

- Specific location, e.g. home, work, etc.
- Mobility pattern, from home, via commute, to work
- Mirroring, two (or more) devices traveling together

NETWORK

- Numbers dialed, (who you call)
- Calls received, (who calls you)
- Calling pattern, (number dialed, for how long, when, how frequently)

PHYSICAL

- IMEI, mobile device ID (the serial number)

- IMSI, mobile subscriber ID (the phone number)

CONTENT

- Identifiers, e.g. names, locations
- Voice fingerprinting
- Keywords

SMARTPHONES

- Ad network analytics
- GPS
- Apps scrape and upload content
- Mothership pings
- Android ID
- MAC address

SMARTPHONES CONT.

- IP address
- WiFi beacons
- Cameras
- Gait analysis (via sensors)

THREAT MODEL

LOCAL SECURITY FORCES

- Reporters are searched and interrogated
- AJ reporters arrested for “spy equipment”
- Mobile 3G access point
- Militia members thought it looked “suspicious”

NOT NSA

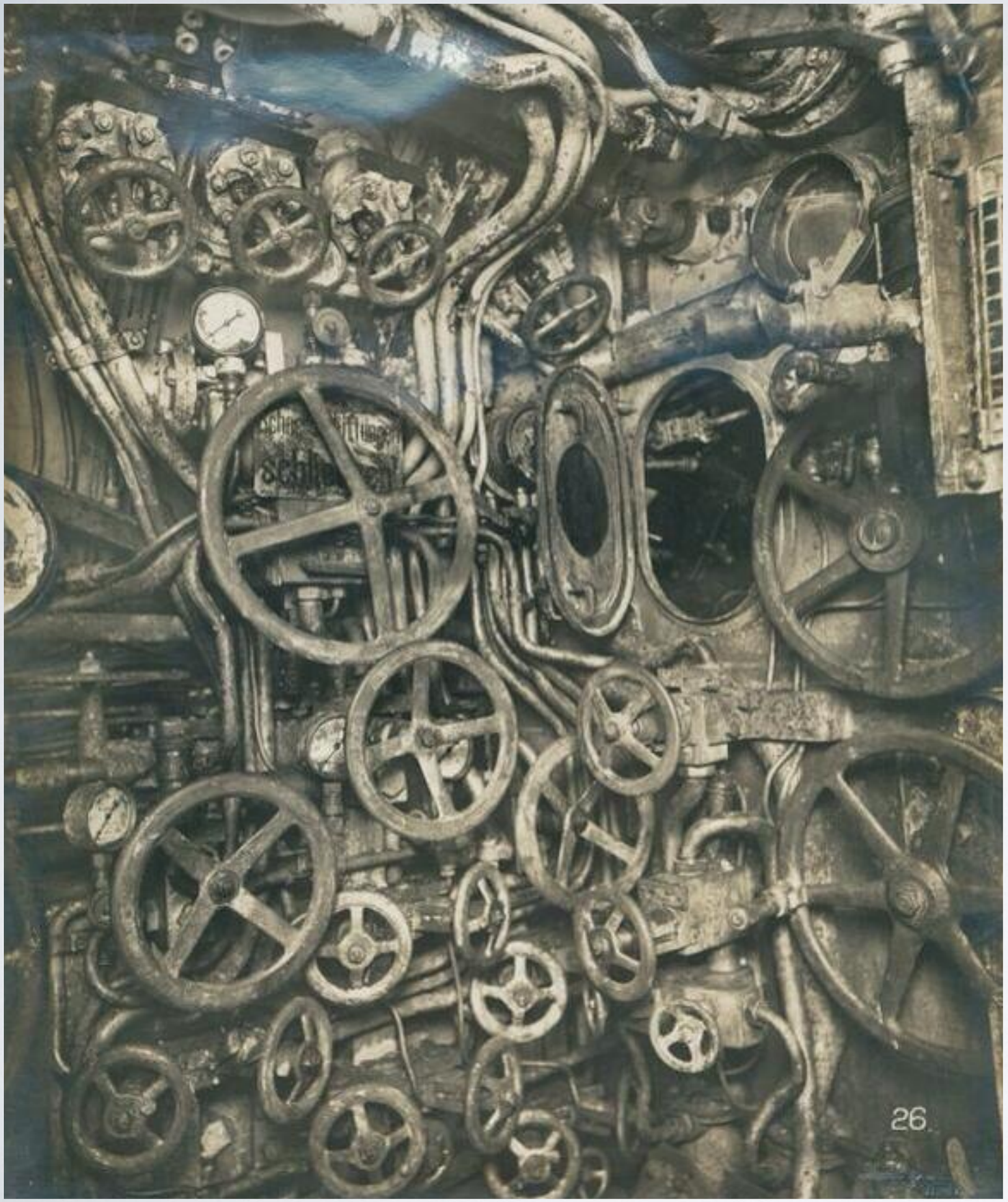
USERS

SECURITY IS HARD WORK

SECURITY TAKES DISCIPLINE

USERS ARE LAZY

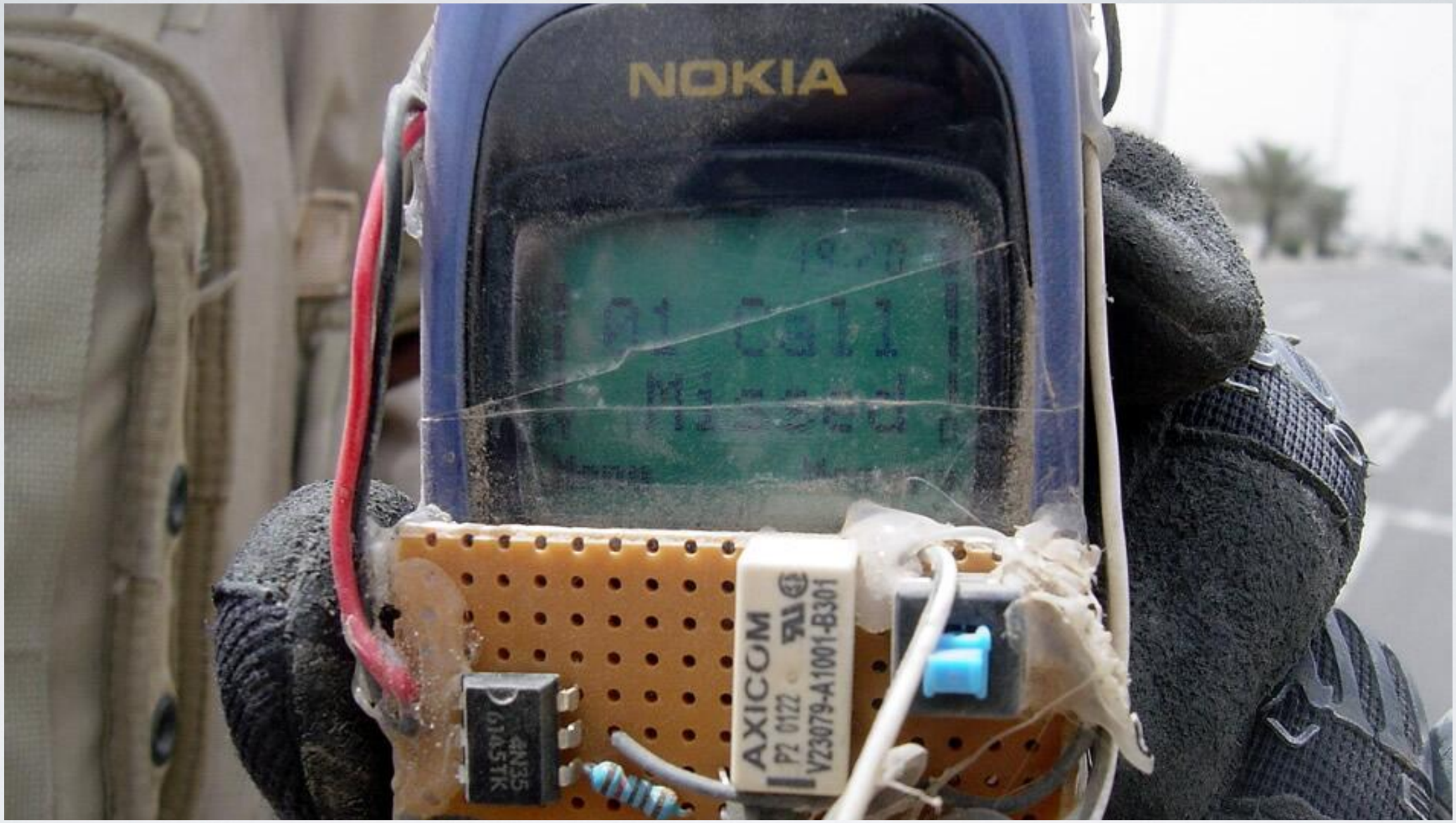
so are we



EASY TO USE

SECURE BY DEFAULT

REASONABLY SECURE



BURNER PHONES

WHAT ARE THEY GOOD FOR?

- Threat actors without nation state level capabilities
  - Your mom
- Building a non-operational legend
  - Flesh out a persona that doesn't need protection

DEFINITELY NOT NSA

BURNER GUIDELINES

- Dumber the better
- Learn to disable completely (battery + SIM out)
- Disable around locations linked to you (home!)
- Never put in real information
    - Feel free to load with fake data

https://b3rn3d.herokuapp.com/blog/2014/01/22/burner-phone-best-practices/

BURNER GUIDELINES, CONT.

- Call non-operational numbers to chaff the analysis
- Keep it short
- Keep it simple
- Get rid of it as soon as possible

BURNER GUIDE CONT.

- Purchase using cash from smaller stores
- Time delay before activation (months)
- Dispose of with extreme prejudice

CLANDESTINE CALLS


DUFFELBLOG
SUICIDAL AL QAEDA
OPERATIVE CALLS
JIHADIST CRISIS LINE

"Never dial [the] number before having thought about your conversation. Do not improvise even the dummy part of it. But do not be too elaborate. The great rule…is to be natural."

–Allen Dulles

- Keep it short, simple and natural
- Prefer signalling over operational data
  - signalling > open codes > plain talk
- Enter your conversation with a plan

"Even if you do not use [the phone] carelessly yourself, the other fellow, very often will, so in any case, warn him."

–Allen Dulles, Former Director of Central Intelligence

FORTRESS PHONE

NSA GUIDELINES

- Two forms of encryption
  - Belts and braces
- Data at rest
  - FDE + app encryption
- Data in motion
  - VPN + app encryption

YOU CANNOT HAVE A SECURE ANDROID PHONE

BECAUSE IT IS A PHONE

BECAUSE IT IS ANDROID

LEO’S LOVE ANDROID

YOU CAN'T BOLT ON SECURITY

Android cannot be secured by adding apps

BUT WHAT IF I…

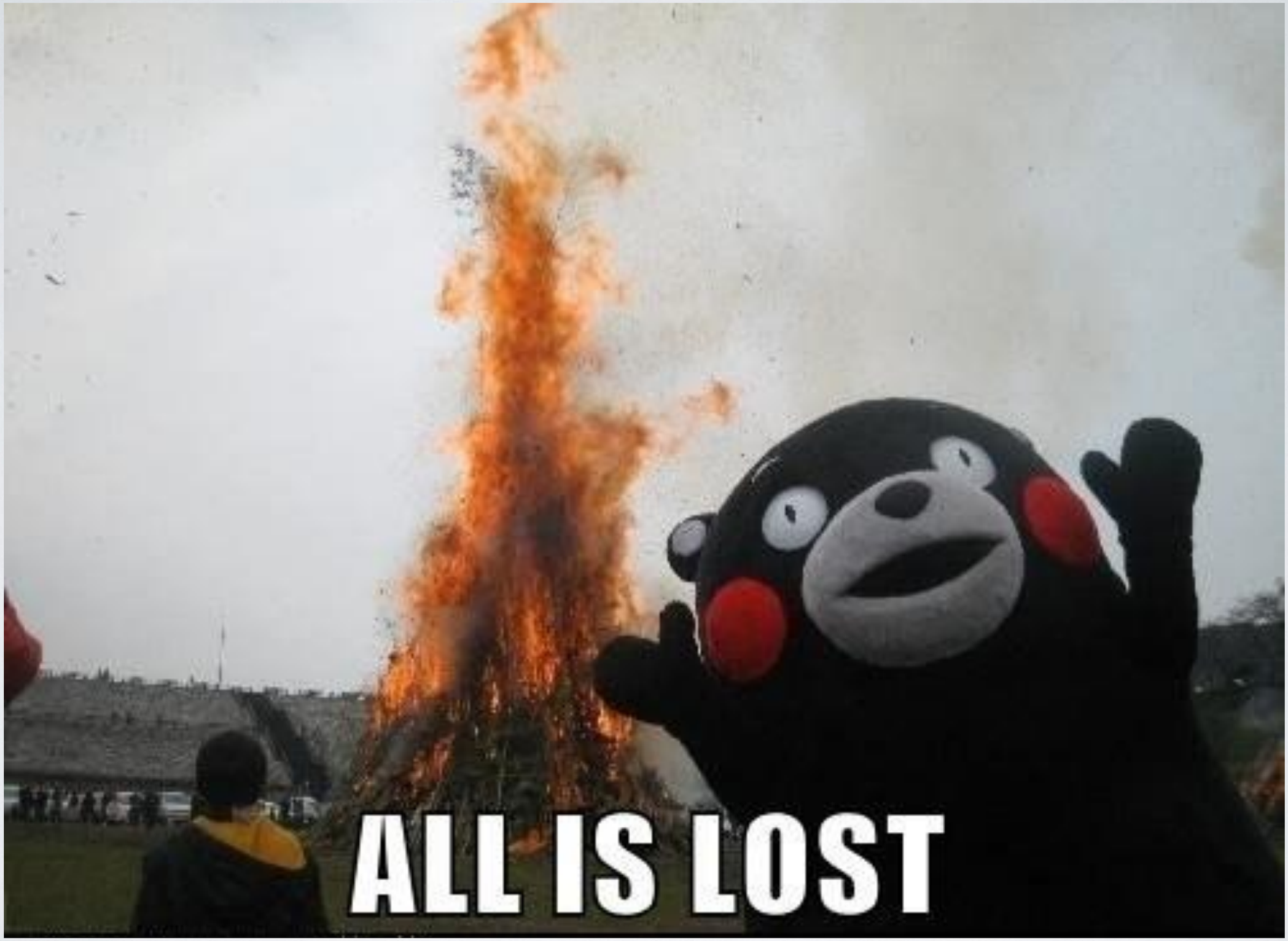
No. Seriously, just no.

- Blackphone
  - For people with money
- Samsung KNOX
  - For people who don’t want a secure phone

- GuardianROM
  - For people who like to reboot
- CryptogenMod*
  - For DIY hackers

* name subject to change

IS IT NSA-PROOF?


ALL IS LOST

CRYPTOGENMOD

Hardened Android ROM

FEATURES

- Lots of crypto
- Robust against physical access
- Resilient against network attacks
- Impact containment

- Derived from CyanogenMod 11
- Stripped down (no browser, no analytics)
- Advanced privacy patches
  - OpenPDroid + PDroid Manager
- Secure application replacements

- Kernel hardening tweaks
  - A lot more work to be done here
- Hardened userland
  - A lot more work to be done here

PROTECTION

- Local physical access
- Remote hacking
- Baseband hacking
- Network monitoring
- GSM monitoring

PHYSICAL

- Forensic analysis
- Encryption
- Security Ratchet

REMOTE

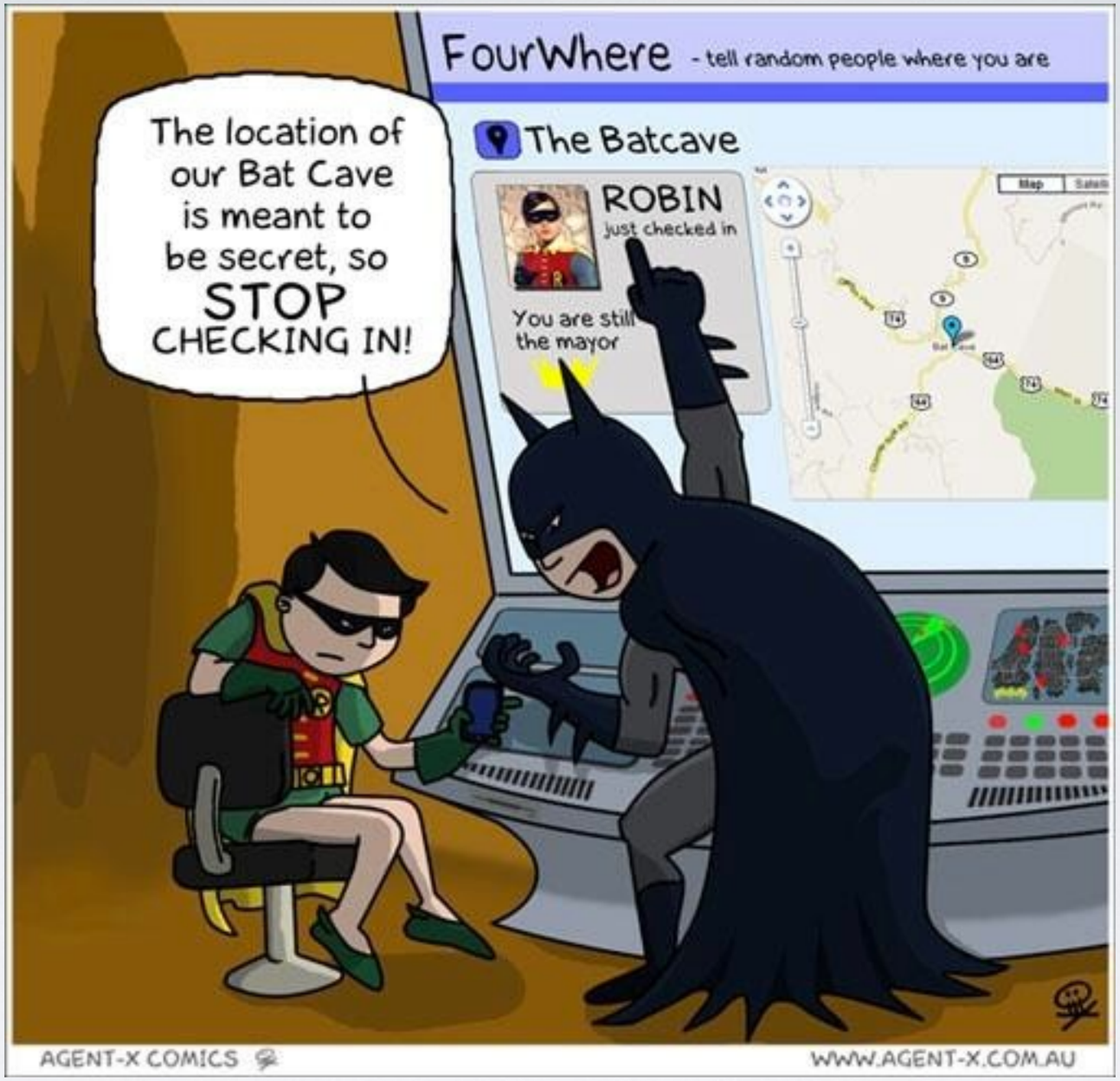
- Reduce attack surface dramatically
  - No browser, services, or email
- No app store

BASEBAND

- Nothing I can do
  - Except PORTAL
- But it's not the end of the world
  - BB exploits are finicky
  - BB design is everything (segmentation FTW)

NETWORK MONITORING

- VPN direct to a secure backend
- Limited information is exposed
- Provides dual layer encryption



OPSEC STILL CRITICAL

Secure phones can’t cure stupid.

DARKMATTER

This App Kills Forensic Analysis

SECURE APP CONTAINERS +

SECURE OPERATIONAL ENV

CRYPTED APP CONTAINERS

MOBILE TRUECRYPT

- Runs apps within TrueCrypt containers
- Automagically kills sensitive apps, then
- mount -o bind … /data/data/$app

MOBILE TRUECRYPT

- tc-play https://github.com/bwalex/tc-play
- Uses the TrueCrypt volume format
  - Supports outer and hidden volumes
- Backend is **dm-crypt** not **FUSE**

MOBILE TRUECRYPT

- Why not use native **/data** encryption?
- AES-256-XTS > AES-128-CBC
- Use both

WIN STATES

CLOSED CRYPTED CONTAINERS

SHUTDOWN/REBOOT COUNTS

HOW DO WE GET THERE?

EVENT BASED HARDENING

CHANGE SECURITY POSTURE BASED ON OBSERVATIONS OF THE OPERATIONAL ENVIRONMENT

- Observe the operational environment
  - Monitor for **SecurityEvents**
- Harden the security posture
  - Trigger **SecurityActions**

INDICATORS OF A NEGATIVE OPERATIONAL ENVIRONMENT

- Failed login
- Timer
- Temperature drop
- Radio silence
- Debugger attach
- Receive alert
- SIM removed

HARDEN SECURITY POSTURE

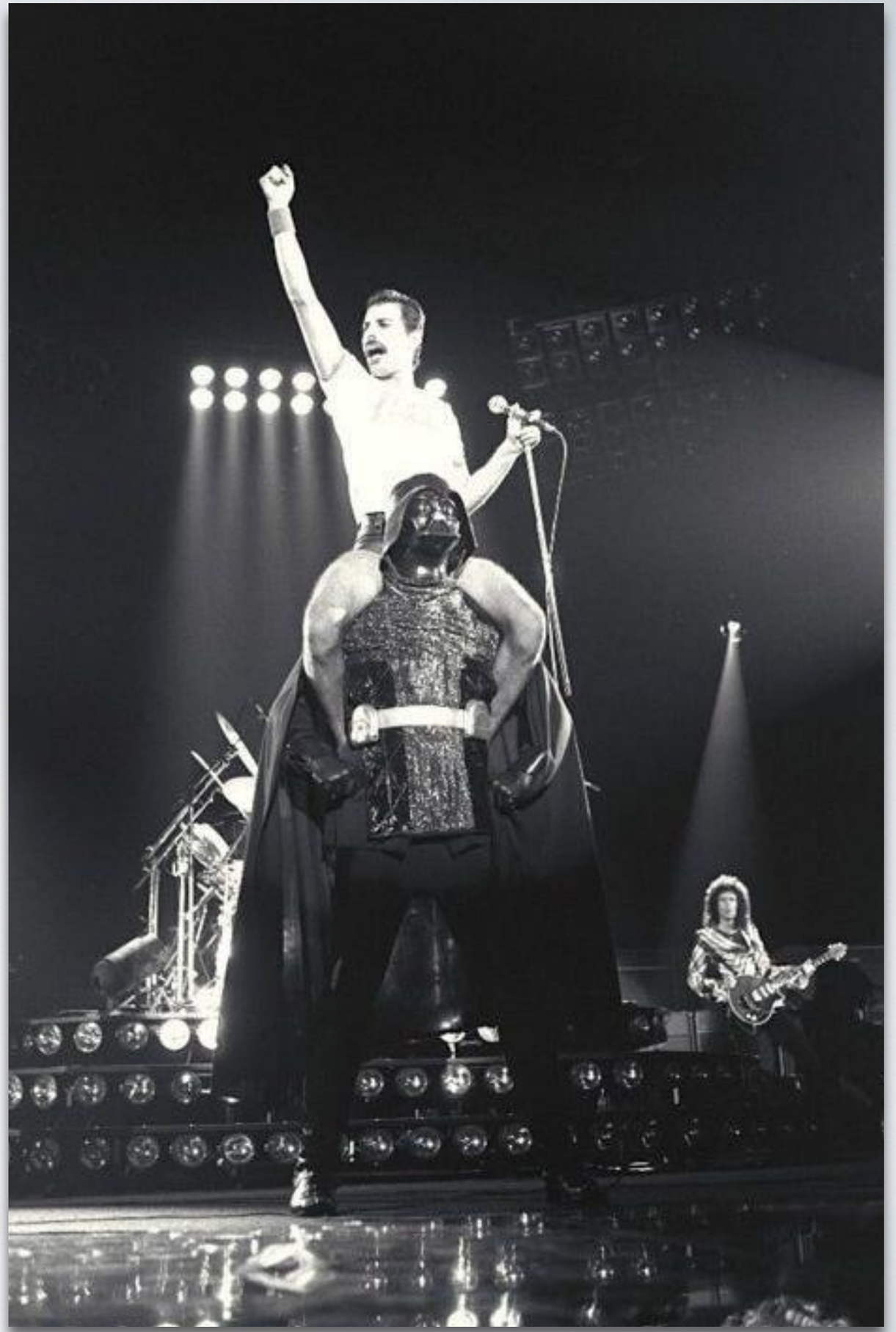
- Kill sensitive applications
- Unmount file systems
- Wipe files
- Wipe ram
- Reboot phone

DURESS CODES

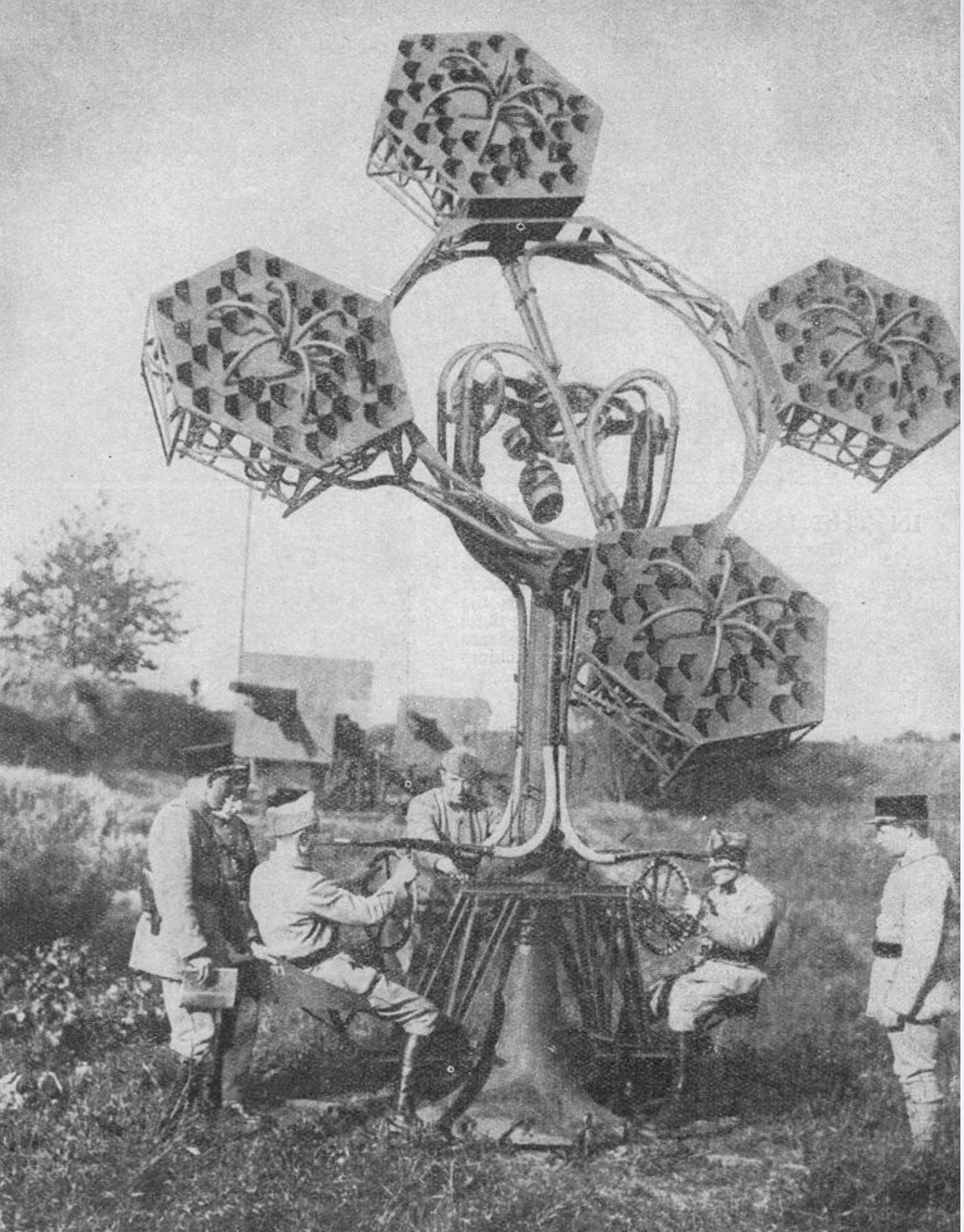
- Explicit duress codes don't work
- "of these two codes, only use this one when you're under extreme stress. ps don't forget"
- "if you use the wrong code, you are severely punished"

CryptogenMod +

DarkMatter =

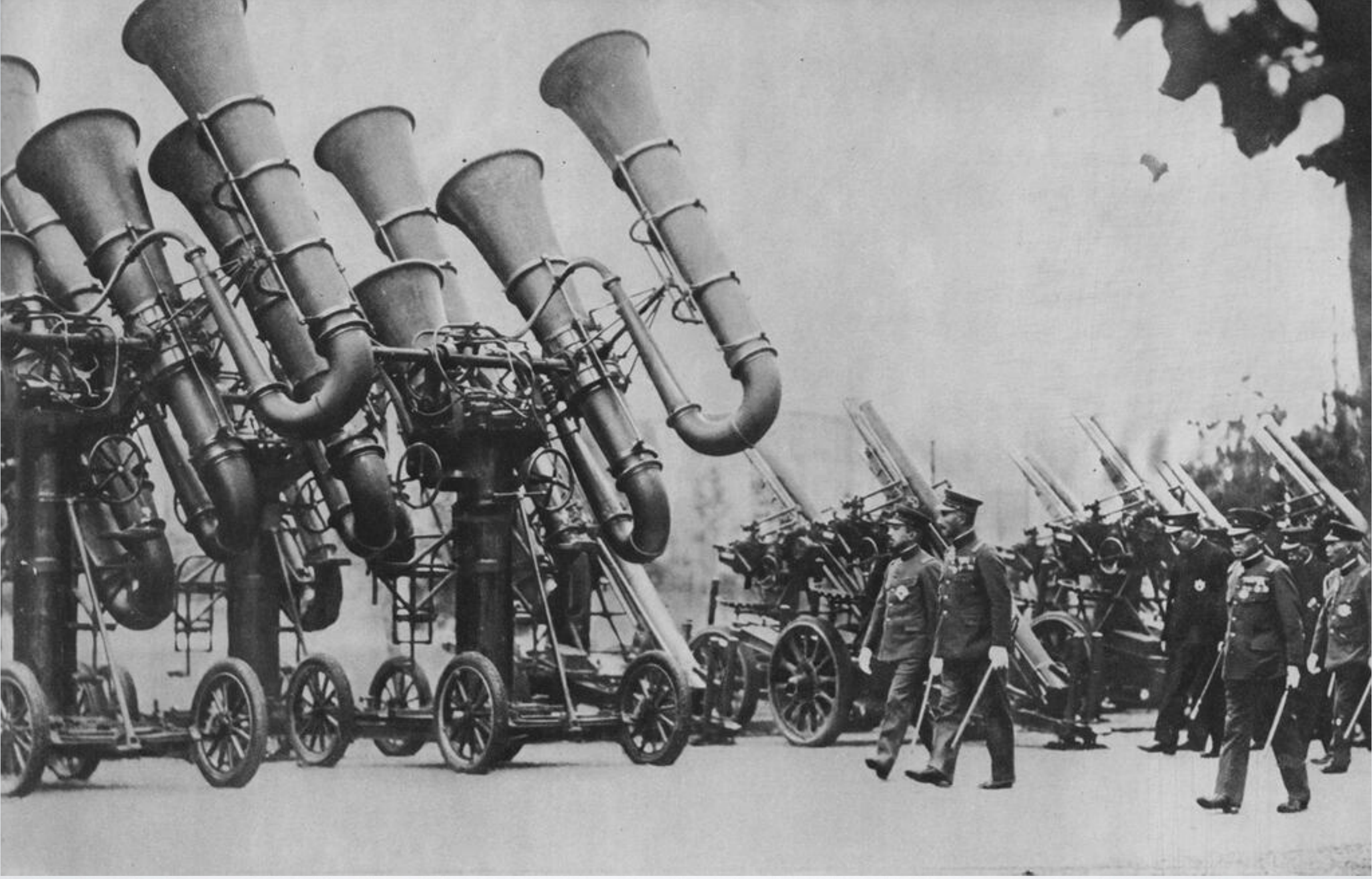


http://github.com/grugq/darkmatter



RAISE
NSA
PRICE 2 PWN*

* probably



THEY'LL ADAPT

Journalists, media under attack from hackers: Google researchers

BY JEREMY WAGSTAFF

SINGAPORE Fri Mar 28, 2014 5:48am EDT

THANKS!


WE WANT BEER
WE WANT BEER
WE WANT BEER
WE WANT BEER
WE WANT BEER
WE WANT BEER

QUESTIONS?

THANK YOU

@thegrugq

the.grugq@gmail.com