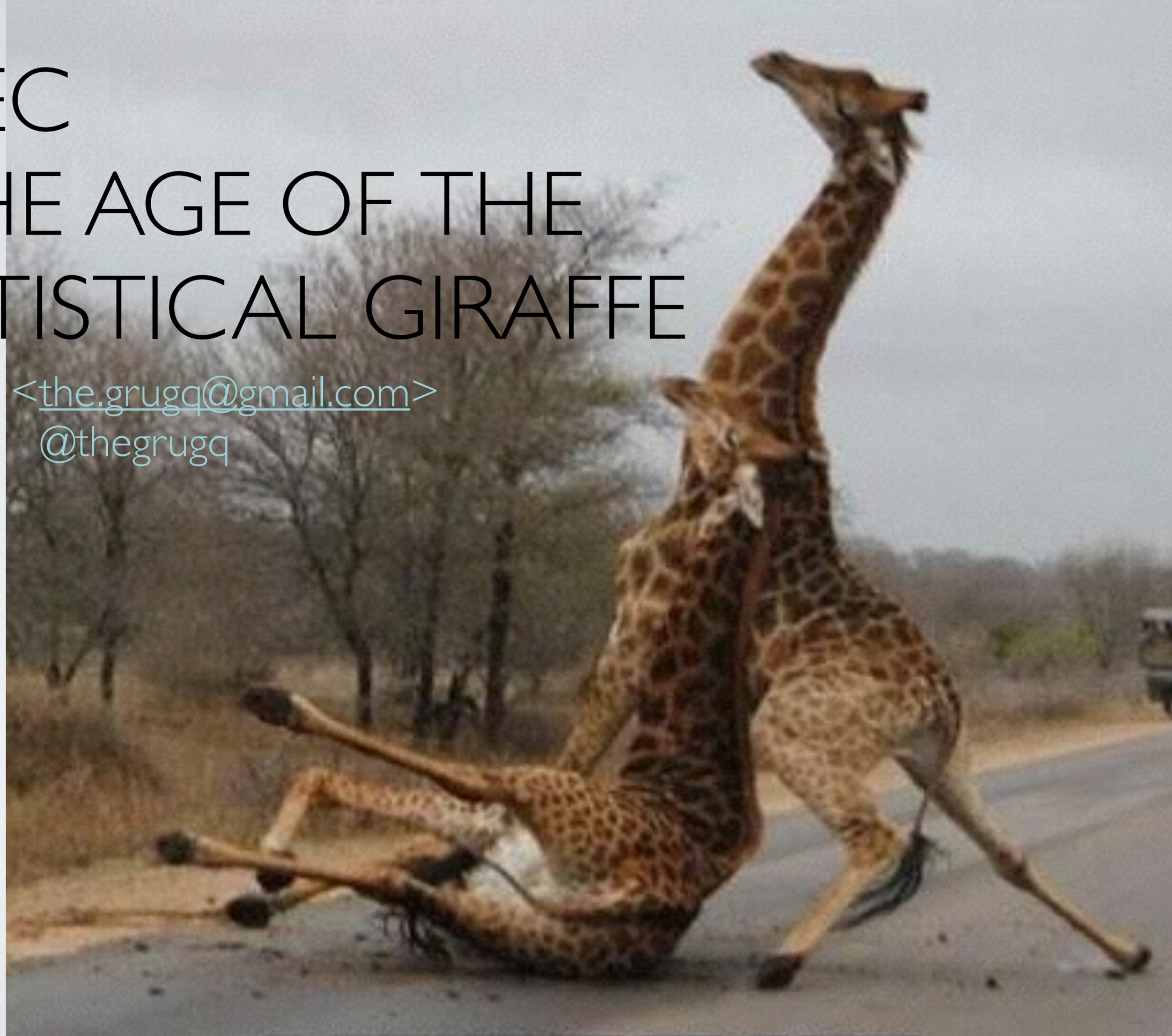
OPSEC IN THE AGE OF THE EGOTISTICAL GIRAFFE

the grugq <the.grugq@gmail.com>
@thegrugq

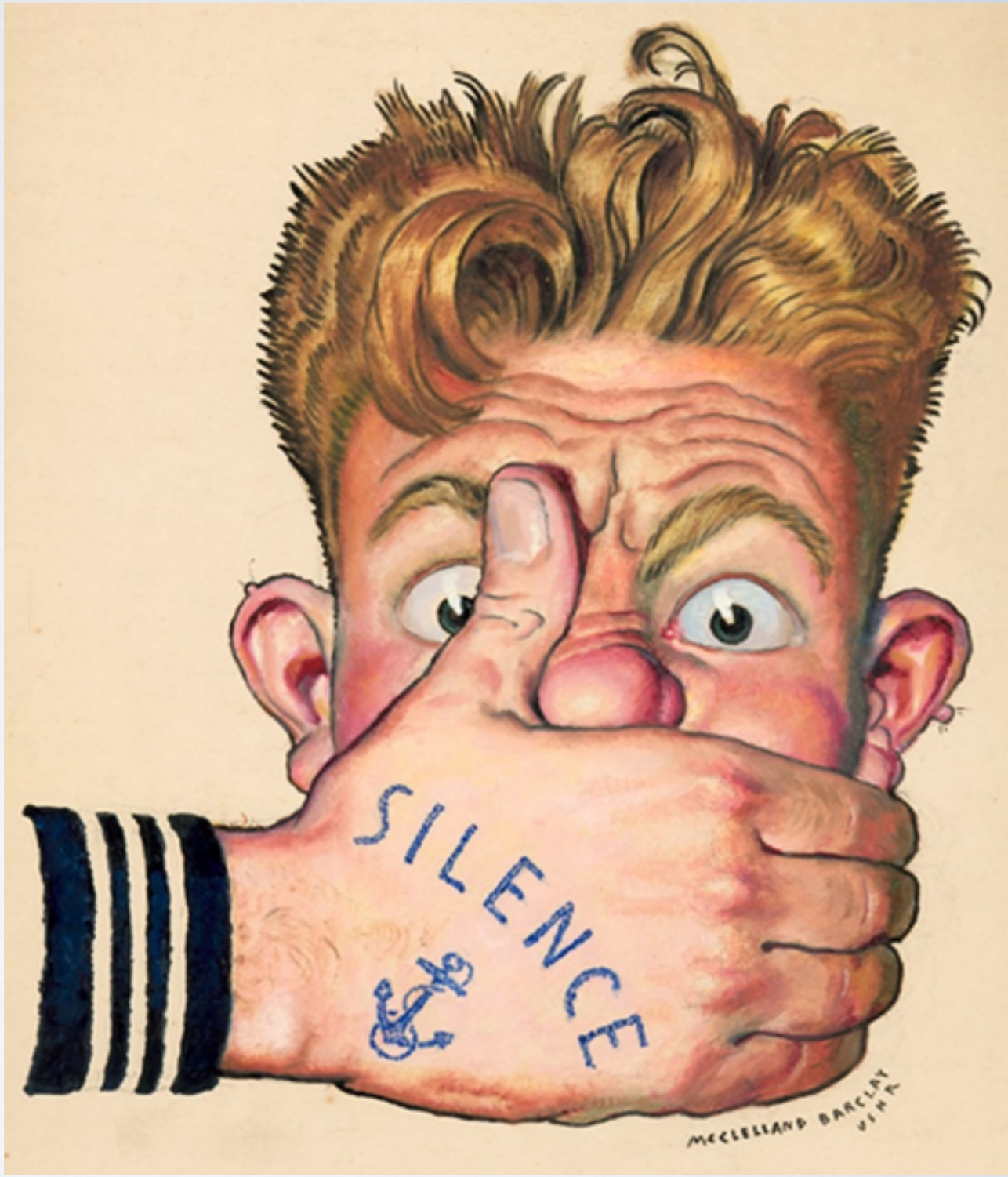


EGOTISTICAL GIRAFFE

- 0day exploit against Firefox browser
- Targeted at Tor Browser Bundle users
- Similar to FBI Freedom Hosting malware
- Use a P.O.R.T.A.L.

QUESTIONS?

- Contextualizing 0day
- Lessons Learned
- Mobile Matters
- Tranquil Transmissions



CYBER
CONTEXTUALIZING 0DAY

"Your cyber systems continue to function and serve you not due to the expertise of your security staff but solely due to the sufferance of your opponents."

–Brian Snow, NSA Information Assurance Director

NOT EVERYTHING REQUIRES 0DAY

A FUNCTION OF SECURITY POSTURE AND ATTACK SURFACE

ENTERPRISES

DON’T REALLY NEED 0DAY

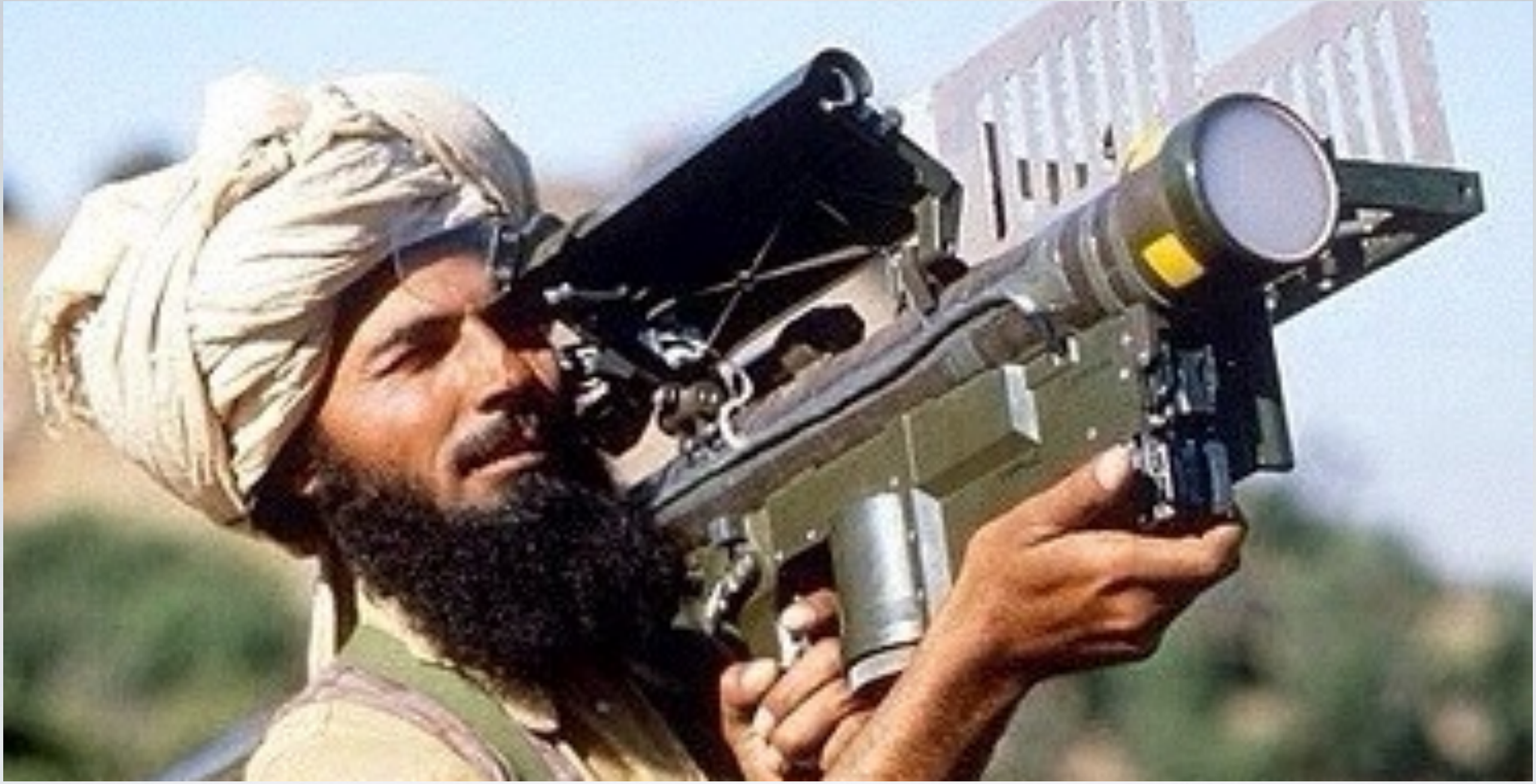
SME

PROBABLY DON’T NEED 0DAY

INDIVIDUALS

MIGHT NEED 0DAY, DEPENDS

NOT EVERYTHING WARRANTS 0DAY



^ DEFINITELY GETTING 0DAY

Phil Venables
@philvenables

Follow

Attackers have bosses and budgets too.

Reply Retweet Favorite ••• More

RETWEETS
35

FAVORITES
25

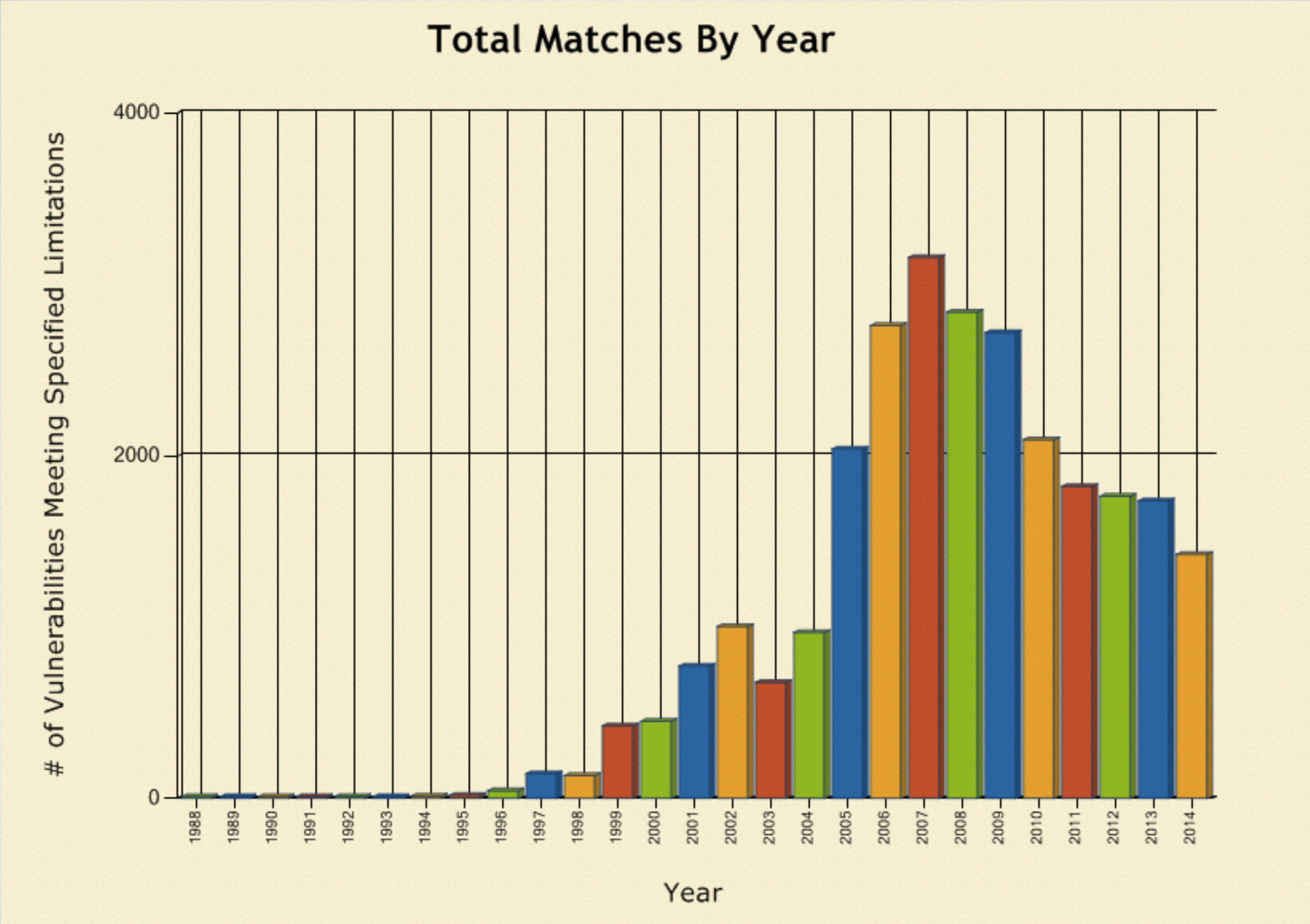
3:01 PM - 13 Sep 2014

ATTACKERS HAVE FINITE RESOURCES

0DAY ARE EXPENSIVE

DOH!DAY ARE CHEAP

0LDAY ARE FREE


Total Matches By Year
# of Vulnerabilities Meeting Specified Limitations
4000
2000
0
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
Year

ATTACKERS NEED RESULTS

"If it's stupid but it works, it's not stupid"

–Murphy's Laws of War

USE PUBLICLY AVAILABLE
ATTACK TOOLS MADE BY OTHERS
GET LABELED A 'SOPHISTICATED' THREAT

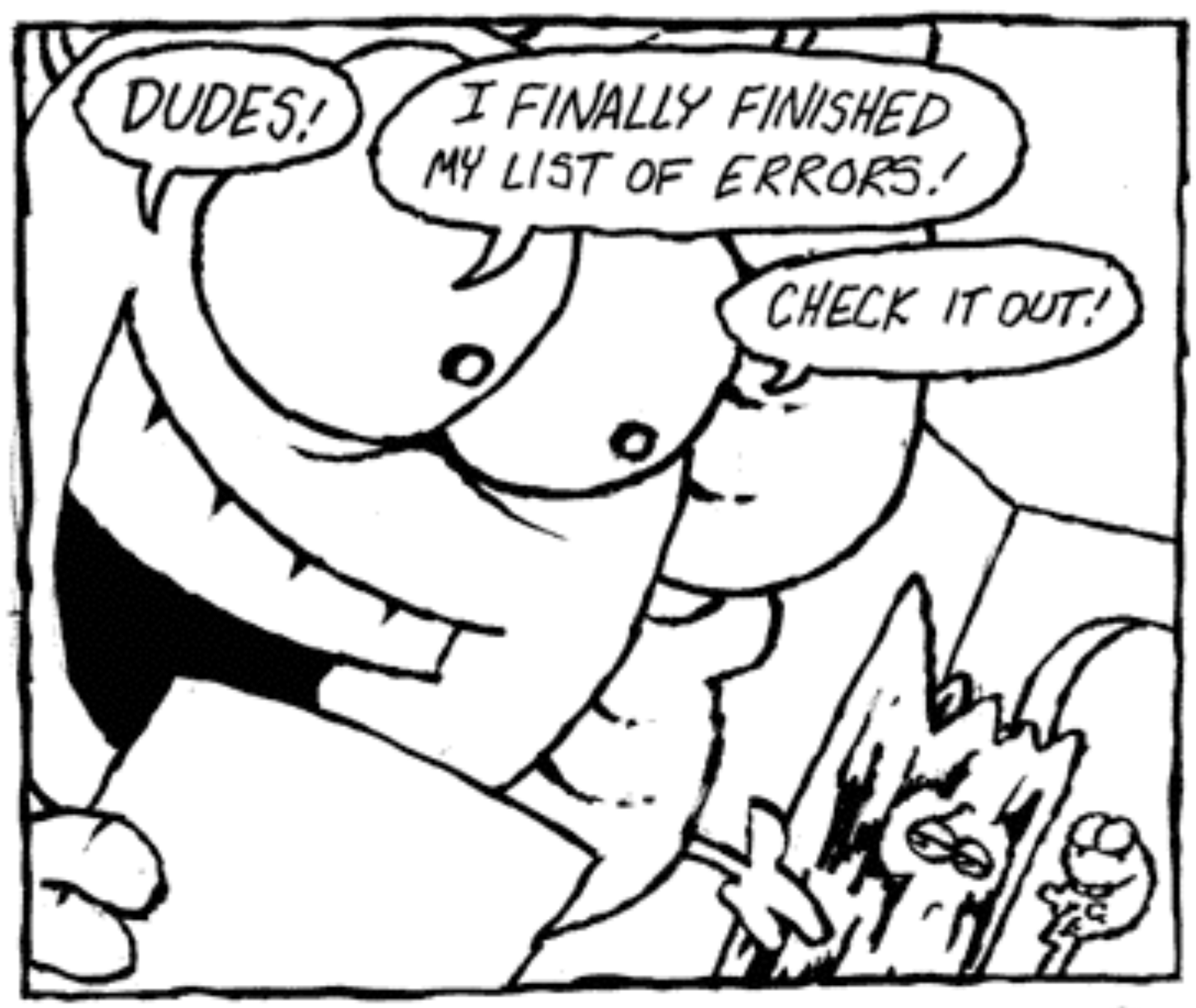
WHAT IF THE SOPHISTICATED ATTACKERS
WHO USE COMMONLY AVAILABLE TOOLS
CAN'T ACTUALLY DO ANYTHING BETTER?

ENTERPRISE SECURITY PROTIP

ENTERPRISE SECURITY

- Attack surface is too big
- Trust relationships too diverse and complex
- Security posture inconsistent
- Essentially unsolvable
  - Compartment and secure something smaller

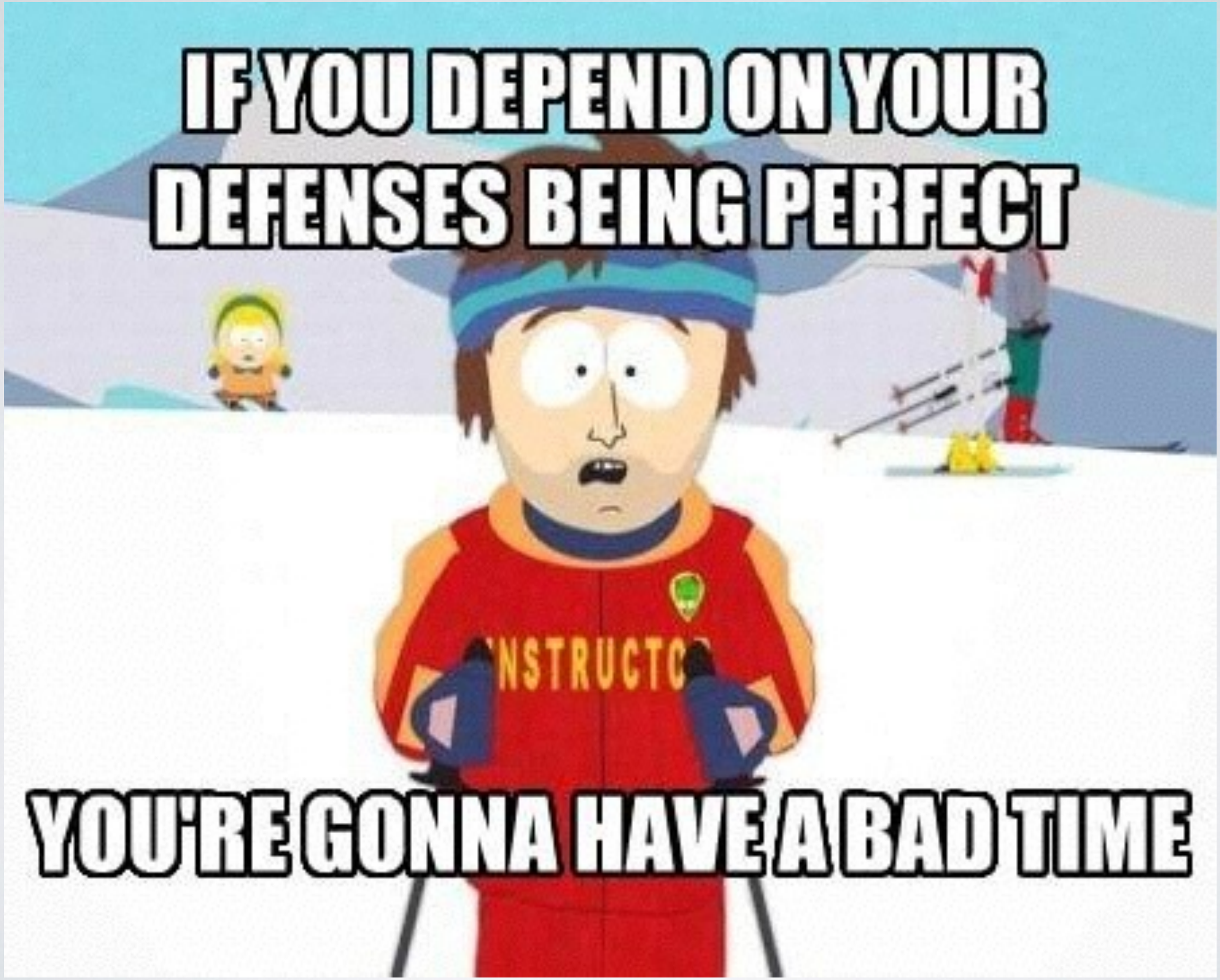
LESSONS LEARNED


DUDES!
I FINALLY FINISHED MY LIST OF ERRORS!
CHECK IT OUT!

MY LIST:
-nope

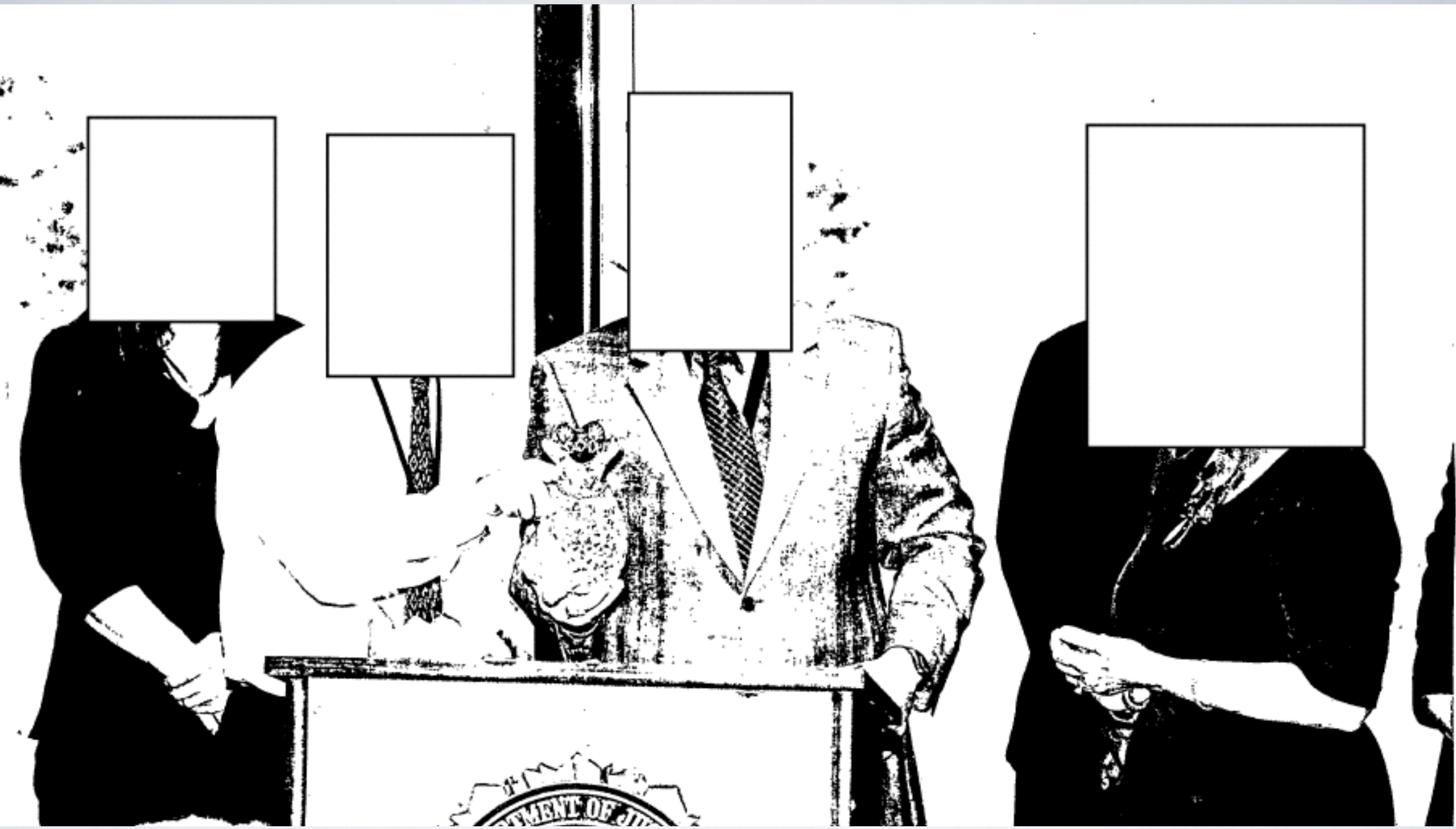
FEELS SO GOOD!
CONFIRMING THAT I'VE BEEN IN THE RIGHT ON EVERY SINGLE OCCASION?
SUPER LIBERATING!

WORSE THAN WE THOUGHT


IF YOU DEPEND ON YOUR
DEFENSES BEING PERFECT
YOU'RE GONNA HAVE A BAD TIME

BECAUSE

VUPEN



OPSEC STILL WORKS

IF YOU DO IT PROPERLY

TAKE THAT NSA!
PRIVATE BROWSING!

C'mon son

Rule number one; never trust anybody

Secrets I Keep
From
The Internet

OPSEC WORKS

- Counterintelligence hasn't changed in thousands of years
  - It still hasn't
- The same principles and fundamentals still apply

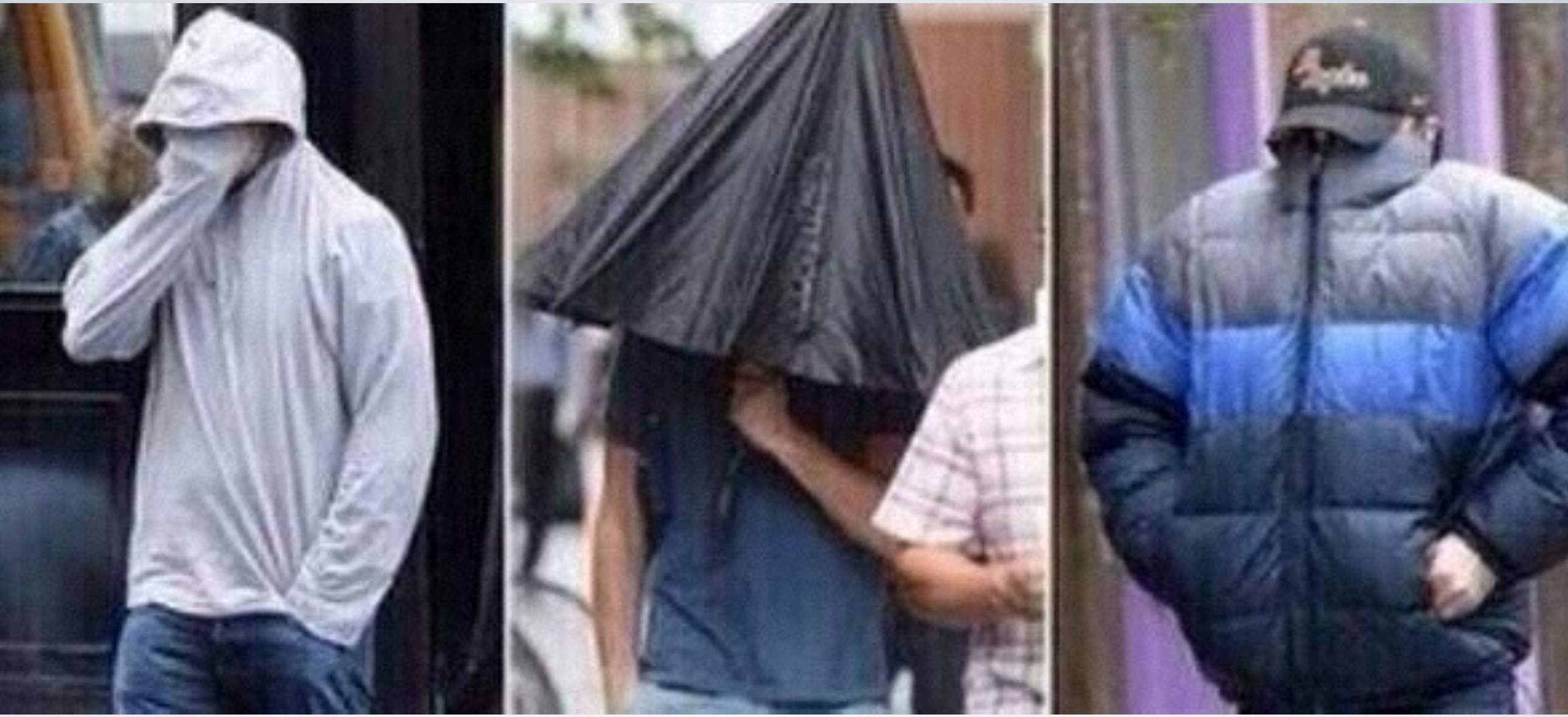
OPSEC: THREE C'S

- Cover
- Concealment
- Compartmentation

COVER

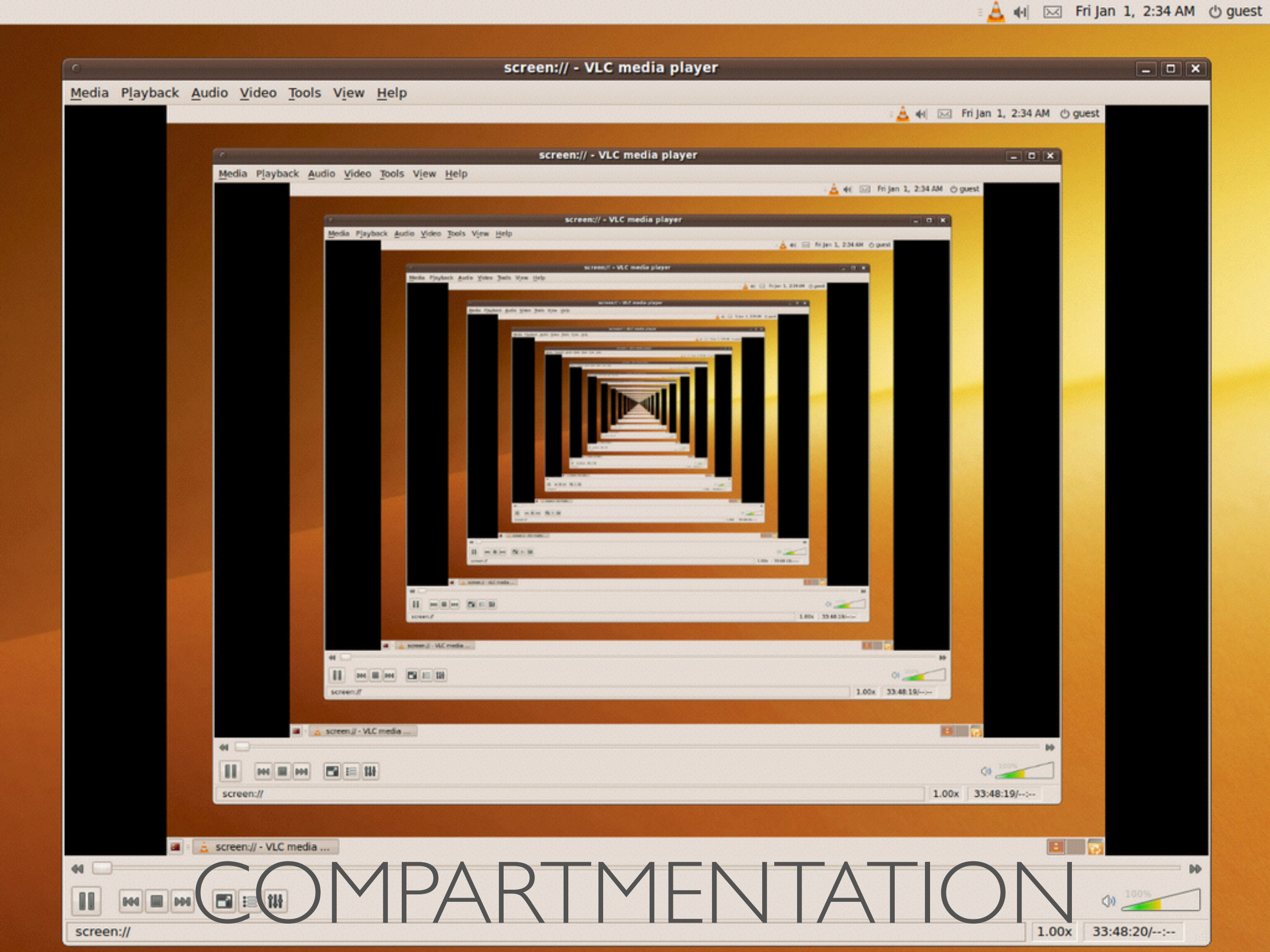
ภท 7379
กรุงเทพมหานคร

- To all appearances, normal
- Cover for Action
  - Normal to do what you are doing
- Cover for Status
  - Normal to be where you are



CONCEALMENT

- Hide the activity
- Prevent anyone from knowing about it
- Hide identities


Fri Jan 1, 2:34 AM
guest
screen:// - VLC media player
Media Playback Audio Video Tools View Help
screen://
1.00x
33:48:20/--:--
COMPARTMENTATION

- Limit the number of people involved
  - Reduce chance of leakage
- Limit scope of the damage if it goes wrong
    - Impact containment
- The last line of defence

SIPR ONLY!!
NIPR ONLY!!
CENTRIX ONLY!!

THE SIZE OF SECRETS

Terrorist Act	# Operatives	Roles of Operatives
Explosives bombing—dropped	1-2	1 bomber, 1 security/driver
Explosives bombing—thrown	1	1 bomber
Explosives bombing—suicide	2	1 bomber, 1 security/driver
Explosives vehicle bomb—suicide	1	1 bomber
Firearms assassination	1-2	1 shooter, 1 backup shooter
Firearms ambush	3+	3 shooters
Explosives ambush	2	1 shooter, 1 lookout/backup
Skyjacking	3-5	1 commander, 2-4 guards
In-flight bomb—dropped	1	1 bomber
In-flight bomb—suicide/martyrdom	1	1 bomber
Arson	1-2	1 arsonist, 1 lookout
Armed raid	5-10+	1 commander, 4-9 shooters
Light infantry weapons attack	3+	1 commander, 2-4 shooters
Surface-to-air missile attack	2	1 lookout, 1 missile launcher
Abduction	3+	1 driver, 2 gunmen/guards

3 things: If you email me please write down the date on all your messages. Second, keep in mind that it takes a few days for emails to get to me so if you are setting an appointment then give me advance notice. Third: you do not need to write "to the sheikh" when you email inspire. Anything from your email will be delivered to me.

Please respond to this message with what you want to say and give it to the brother. We cannot have our brother travel with a laptop plus it is suspicious for you guys to type out a message in a public place.

This brother may be the messenger between us for now. One IMPORTANT note: The brother does not know that he is delivering messages for me and he doesn't know where I am so do not mention that this message is for me. Just give it to him and he will deliver it where it needs to be delivered and will get to me insha Allah.

For future correspondence I believe it would be better if your wife delivers the flash to the brother. It's up to you but I believe that you would definitely be watched and that might put you and the brother in jeopardy. Agree with the brother on the place of meeting. Also we need to keep the meetings to a minimum. The brother says it is not safe for him to enter sanaa frequently. So please mention all what you need to say in the message you send me. Please let me know what your program is and the latest news from the west. Also please send the emails of ikrimah and this other brother with your message.

My wife needs some stuff from sanaa so can your wife buy it for her? We have sent other people before and nothing really suited her taste.

Awlaki's first thumb drive message to me.

OPSEC RULES

"Limit the number of people involved to the bare minimum."

–OPSEC Maxim

"Distance in space and time increases adversarial costs"

–OPSEC Maxim

"When your adversary discovers there's a secret,
the first battle is lost."

–OPSEC Maxim

"Never write if you can speak;
never speak if you can nod;
never nod if you can wink."

–OPSEC Maxim (Martin Lomasney)

"Your adversary has a boss and a budget"

–OPSEC Maxim

"I must not trust.
Trust is the OPSEC killer.
Trust is the fatal error that brings total obliteration."

–OPSEC Maxim

"People make mistakes."

–OPSEC Maxim

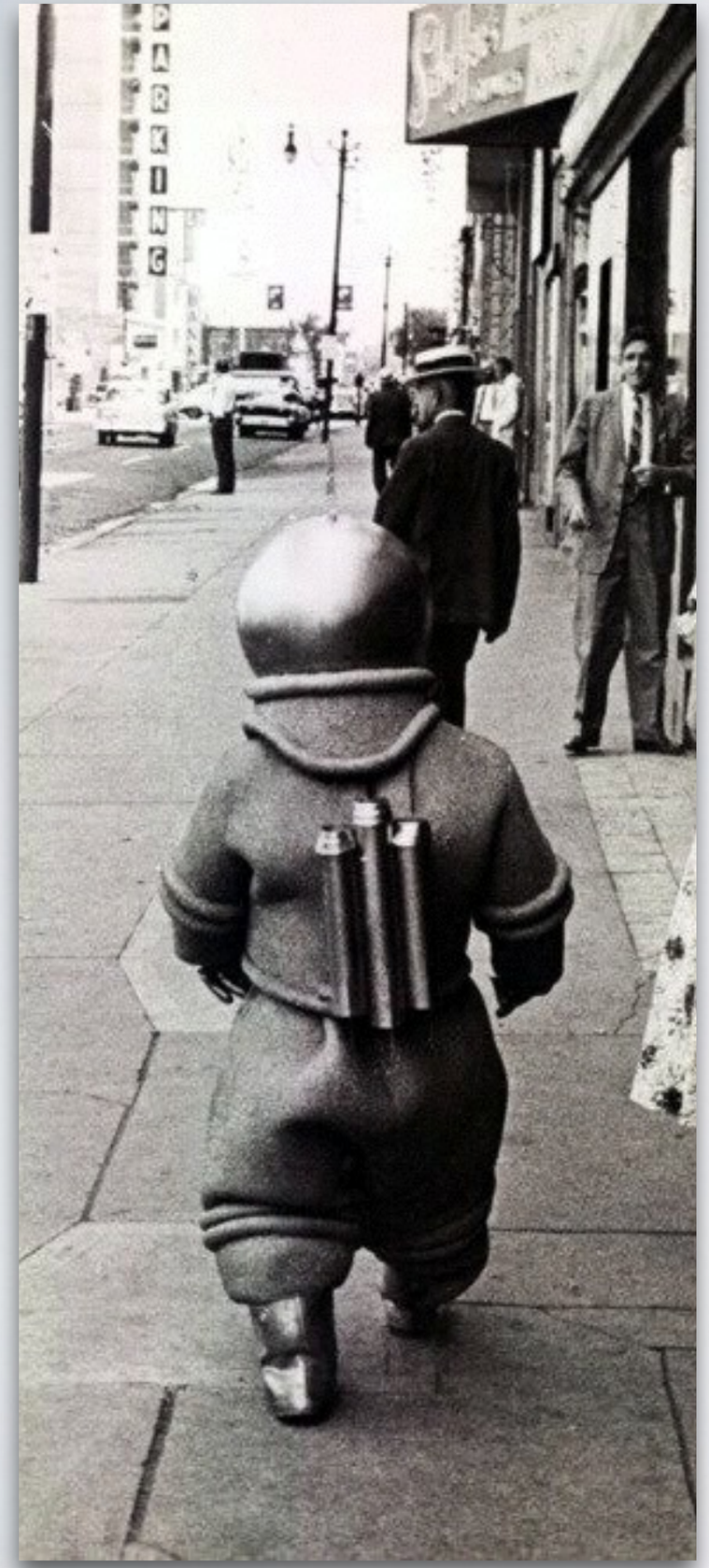
MOBILE MATTERS

SECURE PHONE

UGVvcGxlIG
9uIHRoZSBX
YXNoaW5nd
G9uIFBvc3Q
gRWRpdG9y
aWFsIEJvYX
JkIGFyZSBv
YnZpb3VzbH
kgaWRpb3R
zLg==
Texts
Con
tacts
Pics
Mail
Calls

TACTICOOL PHONES

Galaxy S III (GT-I93
GT-I9500
SM-G900
Nexus 5 (Nexus 5)
Galaxy S III (GT-I81
XT1032
GT-S758
XT1033
Galaxy S Duos (GT
C2104
C230
SM-G7102
Moto X (XT1058)
Nokia_X
GT-I9060
ST26
D55
C1905
GT-S72
SM-T211
D7A+
Lenovo A369
GT-S7580
GT-I9190
GT-S7270
XT918
D6503
S5E
GT-I9105
XT920
ST23
Iris405+
GT-I8
C16
LT30
R821
G-P
A370
R83
A7S
C20
XT925
MS3A
K01
K007
MD
A51
N
XT1
A1
S



STEALTH PHONE

- Secure stealth comms platform

DARKMATTER

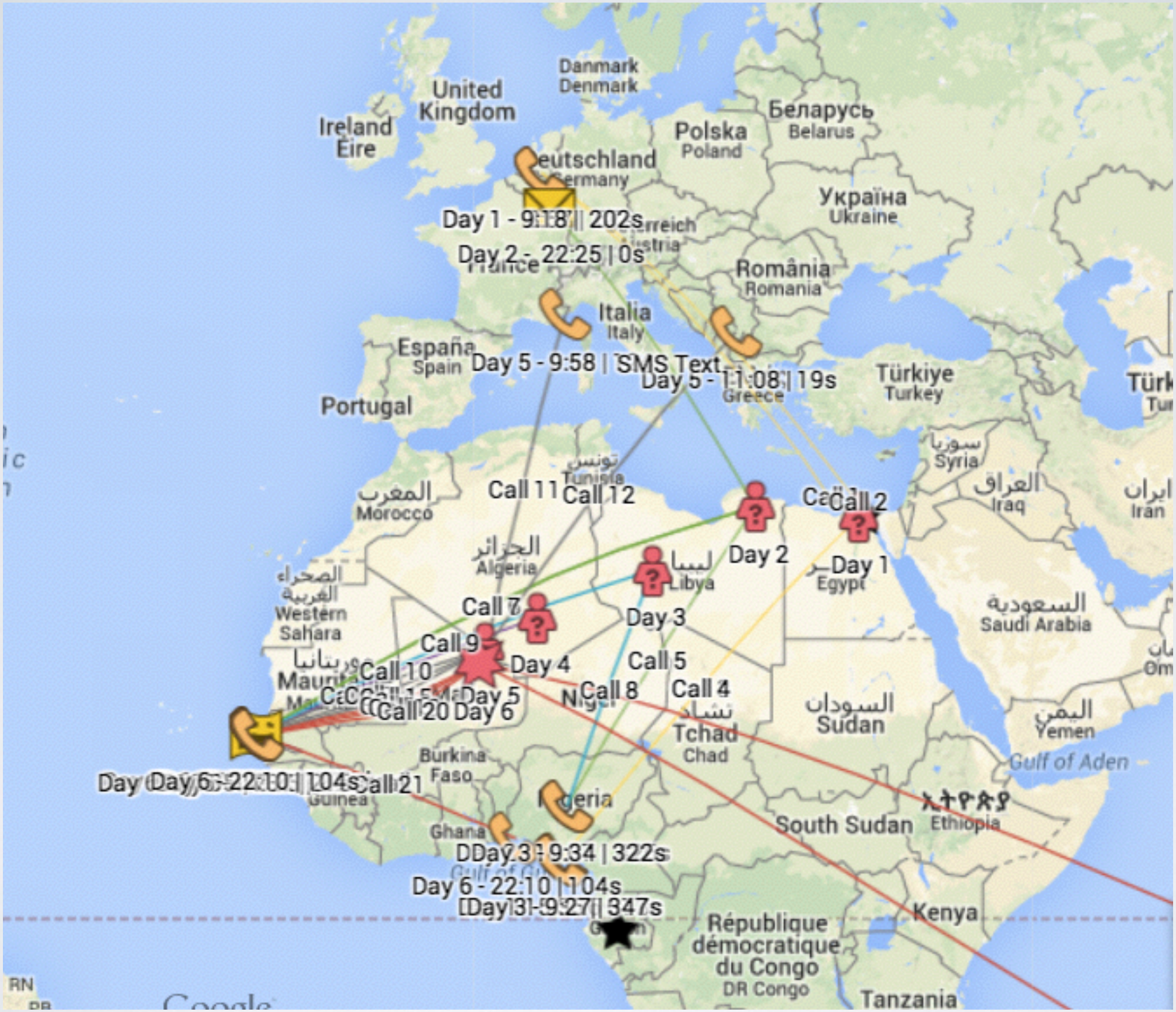
- Secure stealth phone
- Plausible deniability
- Automated hardening
- Active response to attacks

EVENT BASED HARDENING

19 year old Brazilian girl swallows her phone to prevent her boyfriend from reading her texts.

MORE INFO

http://slideshare.com/grugq/mobile-opsec


Danmark
Denmark
United Kingdom
Ireland
Éire
Беларусь
Belarus
Polska
Poland
Deutschland
Germany
Україна
Ukraine
Day 1 - 9:18 | 202s
Day 2 - 22:25 | 0s
France
Österreich
Austria
România
Romania
Italia
Italy
España
Spain
Day 5 - 9:58 | SMS Text
Day 5 - 11:08 | 19s
Greece
Türkiye
Turkey
Portugal
سوريا
Syria
تونس
Tunisia
Call 11
Call 12
Call 1
Call 2
العراق
Iraq
ايران
Iran
المغرب
Morocco
الجزائر
Algeria
Day 2
Day 1
Egypt
ليبيا
Libya
الصحراء الغربية
Western Sahara
Call 7
Day 3
السعودية
Saudi Arabia
Call 9
Day 4
Call 5
Call 10
Call 8
Call 4
Day 5
Call 20
Day 6
Niger
تشاد
Tchad
Chad
السودان
Sudan
اليمن
Yemen
Gulf of Aden
Burkina Faso
Day 6 - 22:10 | 104s
Call 21
Guinea
Nigeria
Ghana
South Sudan
ኢትዮጵያ
Ethiopia
Day 3 - 9:34 | 322s
Day 6 - 22:10 | 104s
Day 3 - 9:27 | 347s
Kenya
République démocratique du Congo
DR Congo
Tanzania

TRANQUIL TRANSMISSION

PGP is error prone

Errors are usually fatal

I JUST INSTALLED MUJAHIDEEN SECRETS
SO I GUESS YOU COULD SAY THINGS ARE PRETTY SERIOUS
memegenerator.net

USING ENCRYPTION STANDS OUT

P.T.T.K.
GALERIA
POLICJA

SECURE ANONYMOUS MESSAGING

POND

- Doesn't rely on Tor
- Designed to resist timing correlations by a GPA
- Not p2p (but anyone can run a server)
- Server knows nothing about clients
  - Can't decrypt anything

- Strong PFS
  - Axolotl ratchet advances every send/reply
- Must be bootstrapped
  - Cumbersome manual KEX
  - “Easy” via a shared passphrase + hookup server

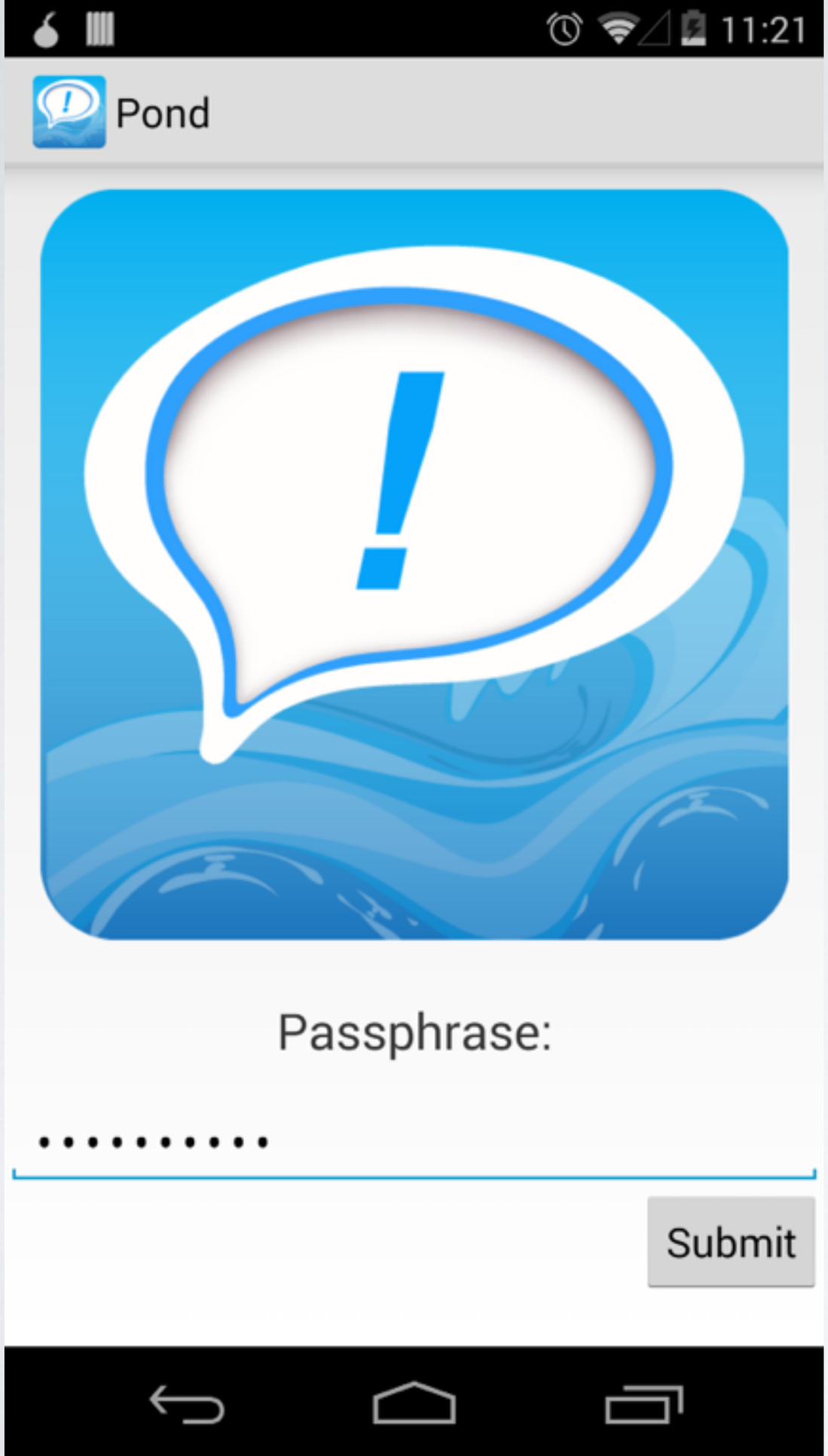
POND IS PURE AWESOME

LETS MAKE IT BETTER

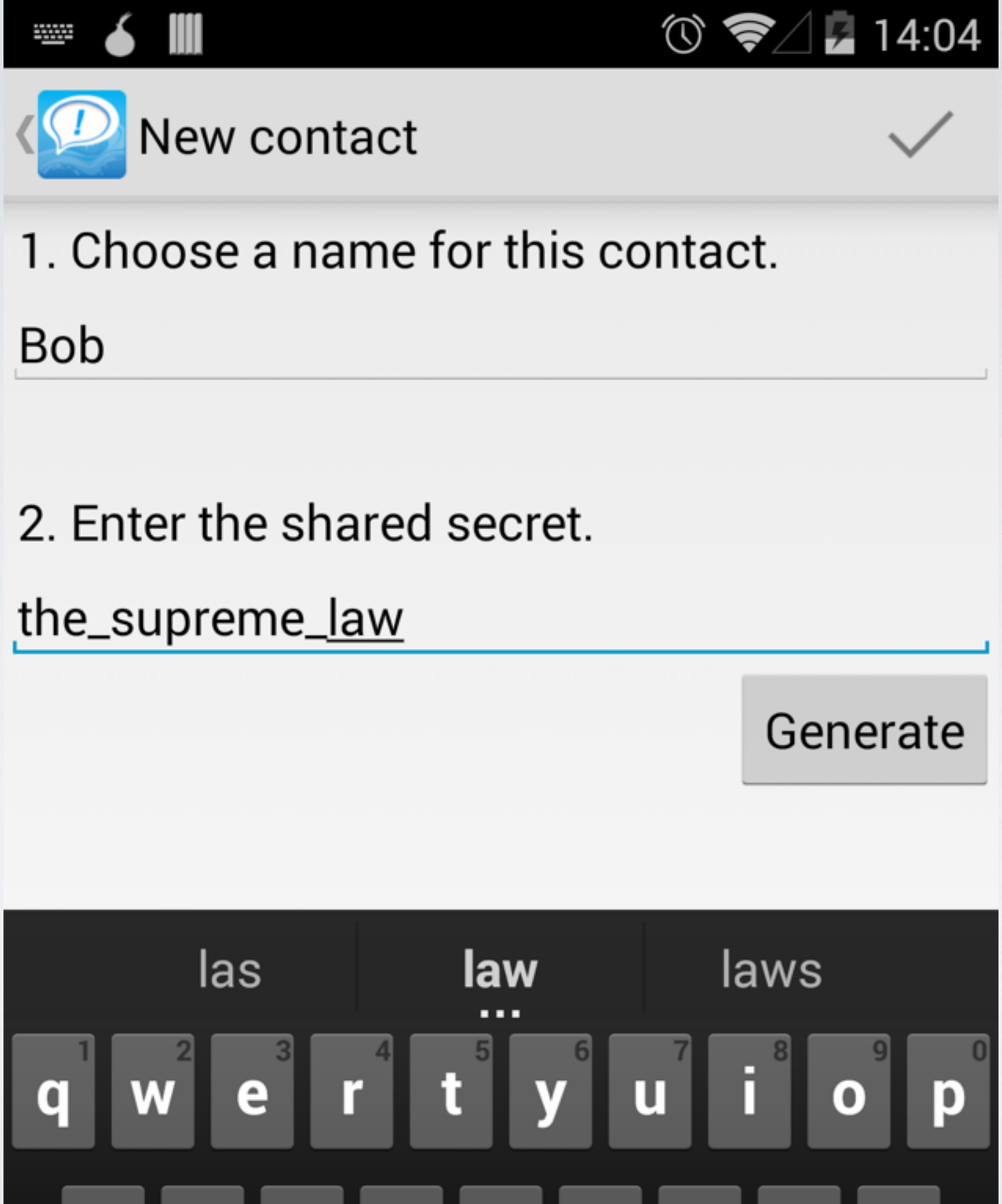
HOW DO WE GET THERE?

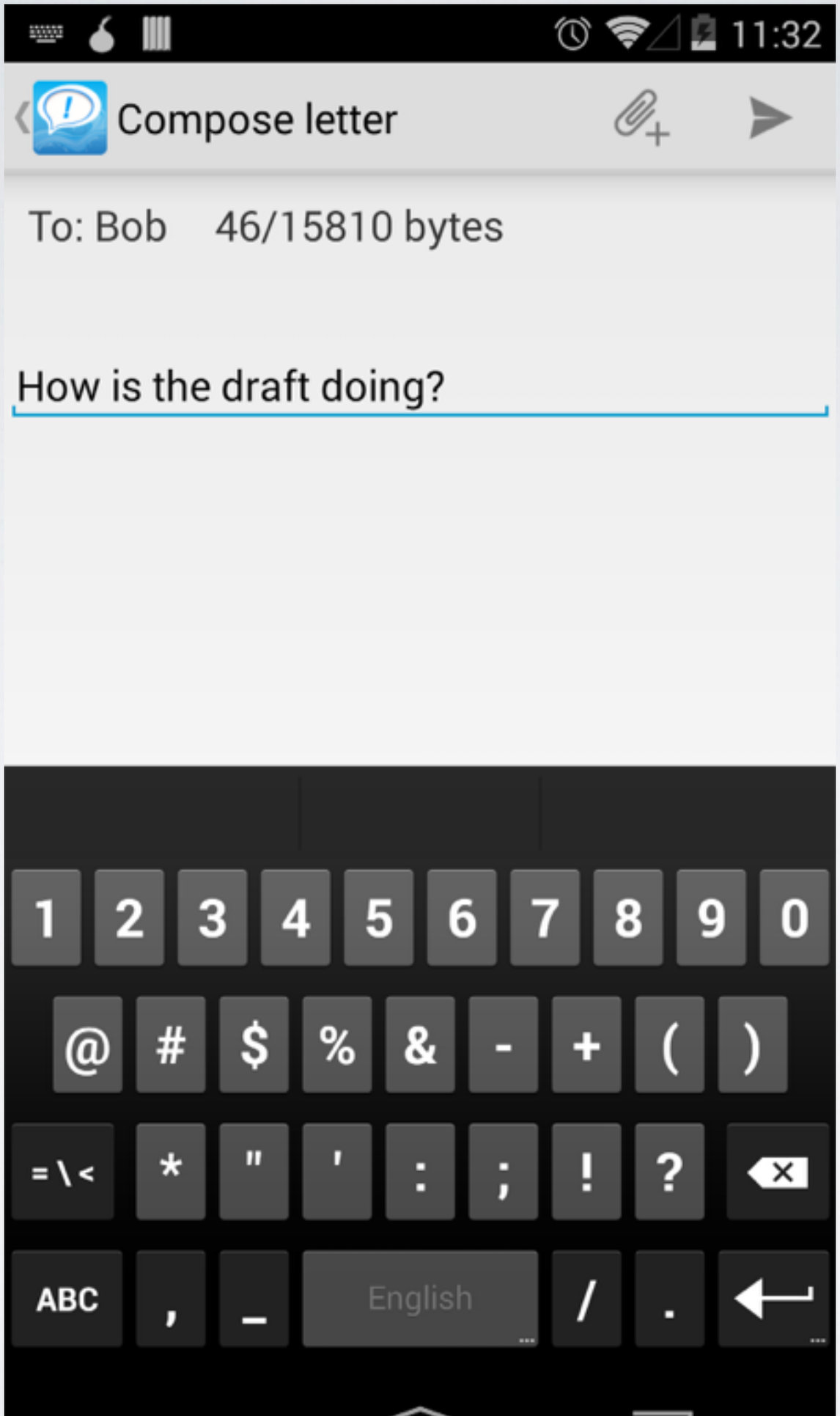
SECURE ANONYMOUS MOBILE MESSAGING APP

DJOOM



POND FOR MOBILE


14:04
New contact
1. Choose a name for this contact.
Bob
2. Enter the shared secret.
the_supreme_law
Generate
las
law
laws


11:32
Compose letter
To: Bob
46/15810 bytes
How is the draft doing?
1 2 3 4 5 6 7 8 9 0
@ # $ % & - + ( )
=\<
* " ' : ; ! ?
ABC
,
English
/
.

11:53

Bob

When in the Course of human events, It becomes necessary for one people to...
We hold these truths to be self-evident, than all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that amon...

13/10/14 11:52

How is the draft going?

13/10/14 11:44

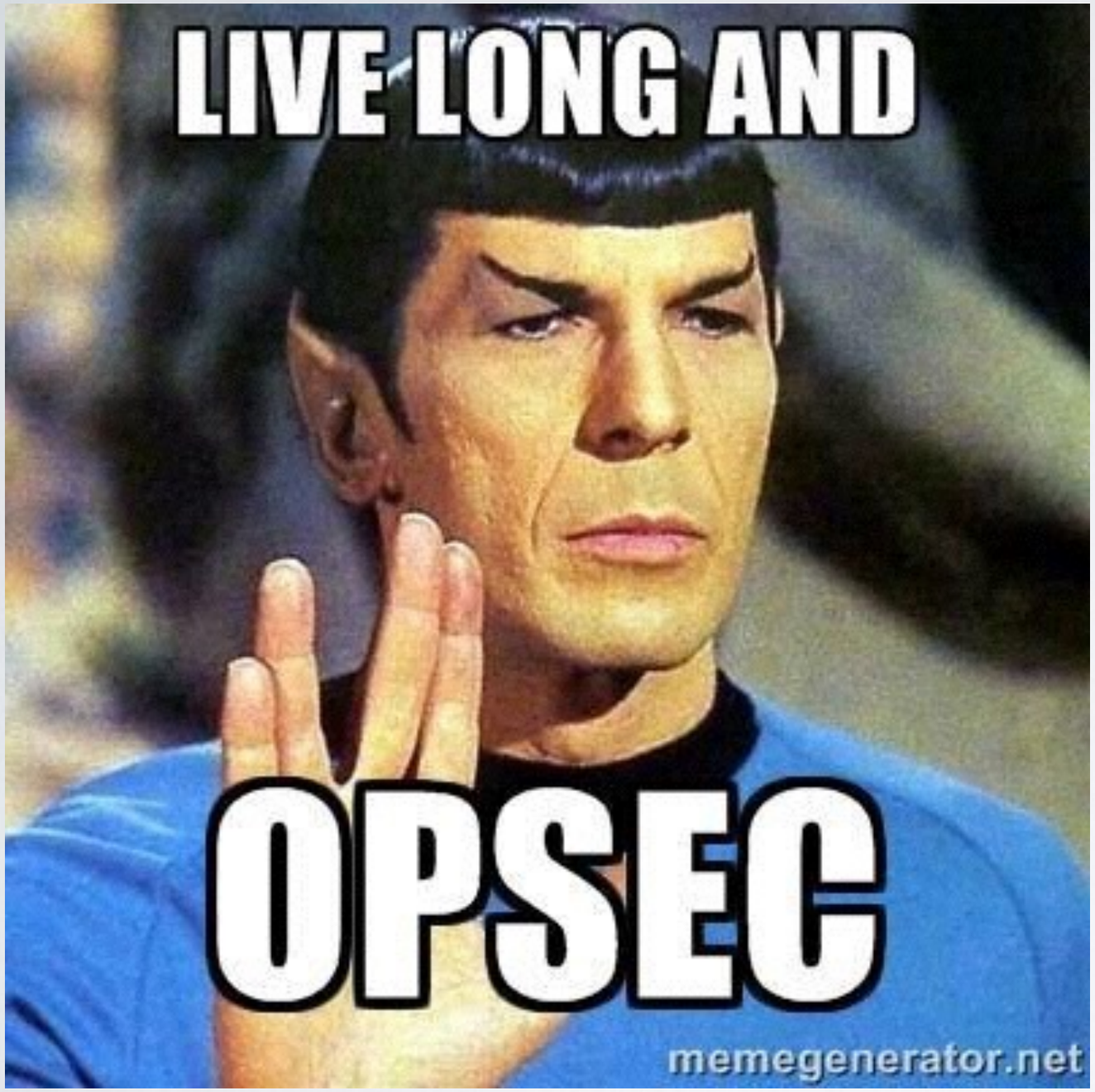
IN GOD WE TRUST
ALL OTHERS WE
MONITOR

Egotistical what?

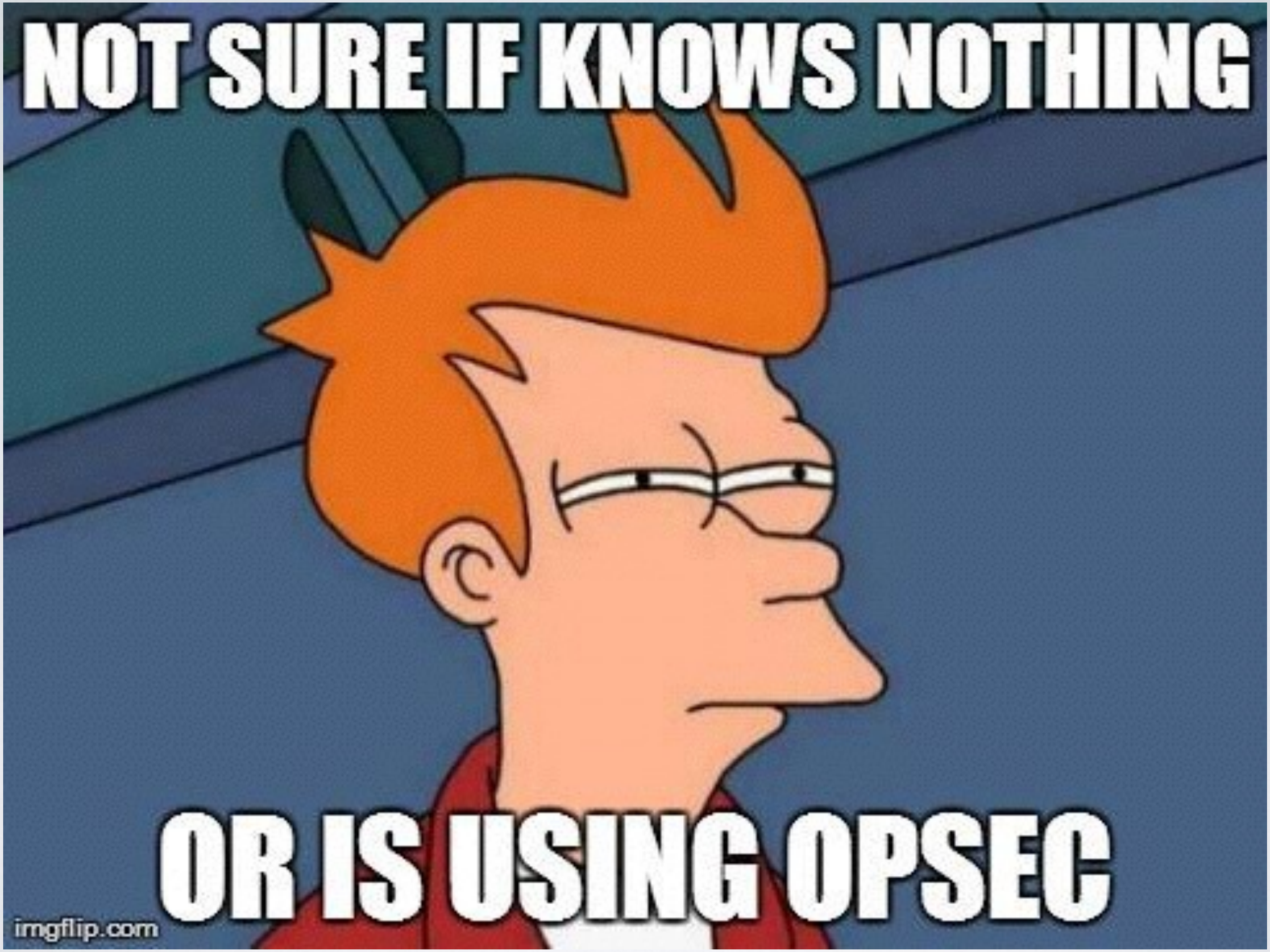
OPSEC MAKES YOU HAPPY

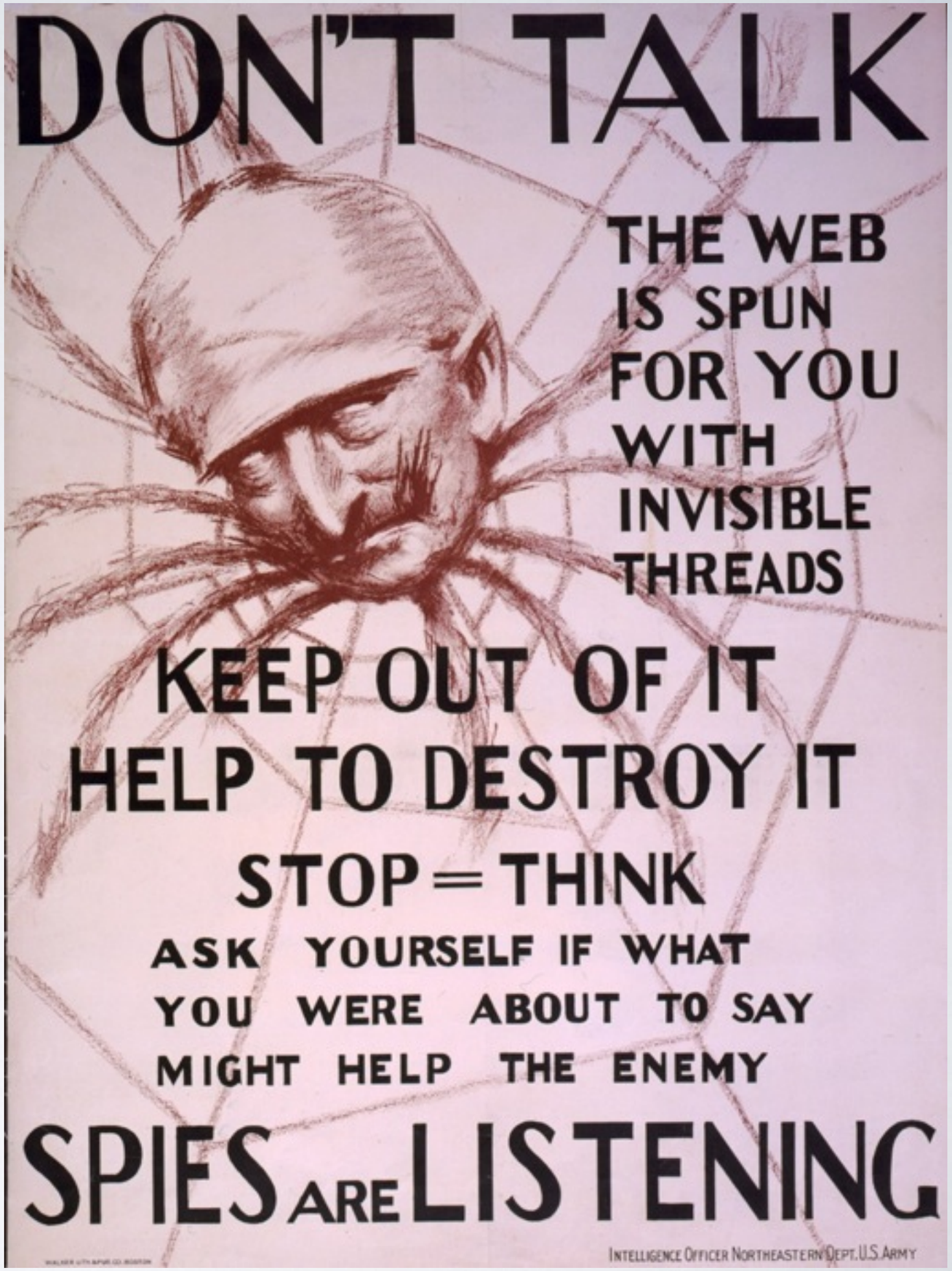
QUESTIONS?

"The ability to speak several languages is an asset, but the ability to keep your mouth shut in any language is priceless."

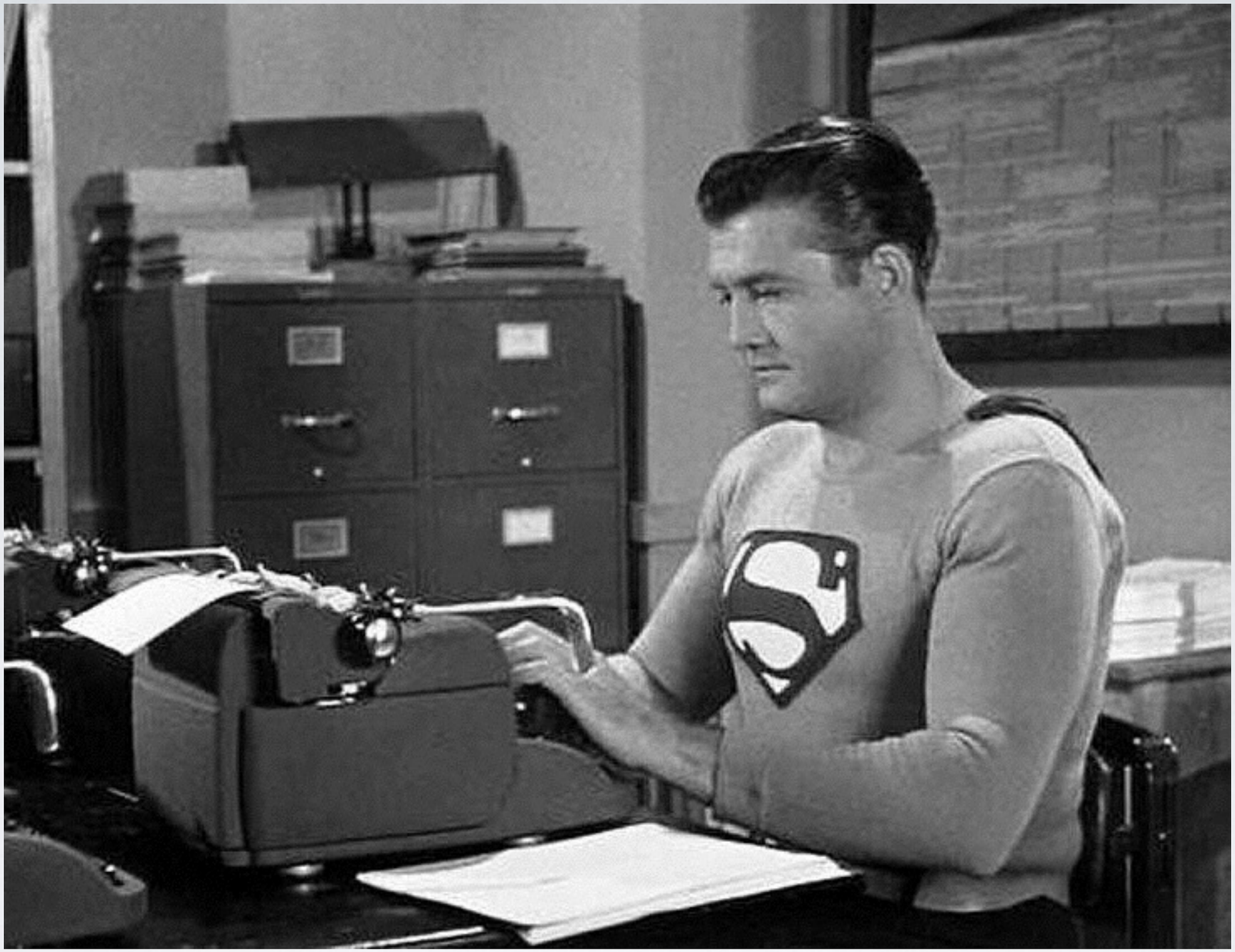


THANKS


NOT SURE IF KNOWS NOTHING
OR IS USING OPSEC
imgflip.com


DON'T TALK
THE WEB
IS SPUN
FOR YOU
WITH
INVISIBLE
THREADS
KEEP OUT OF IT
HELP TO DESTROY IT
STOP = THINK
ASK YOURSELF IF WHAT
YOU WERE ABOUT TO SAY
MIGHT HELP THE ENEMY
SPIES ARE LISTENING
INTELLIGENCE OFFICER NORTHEASTERN DEPT. U.S. ARMY

BLASTED COMPUTER! HERE, EAT IT, YOU JOB-CONSUMING, TRANSISTORIZED, OVER-INFLATED ADDING MACHINE!

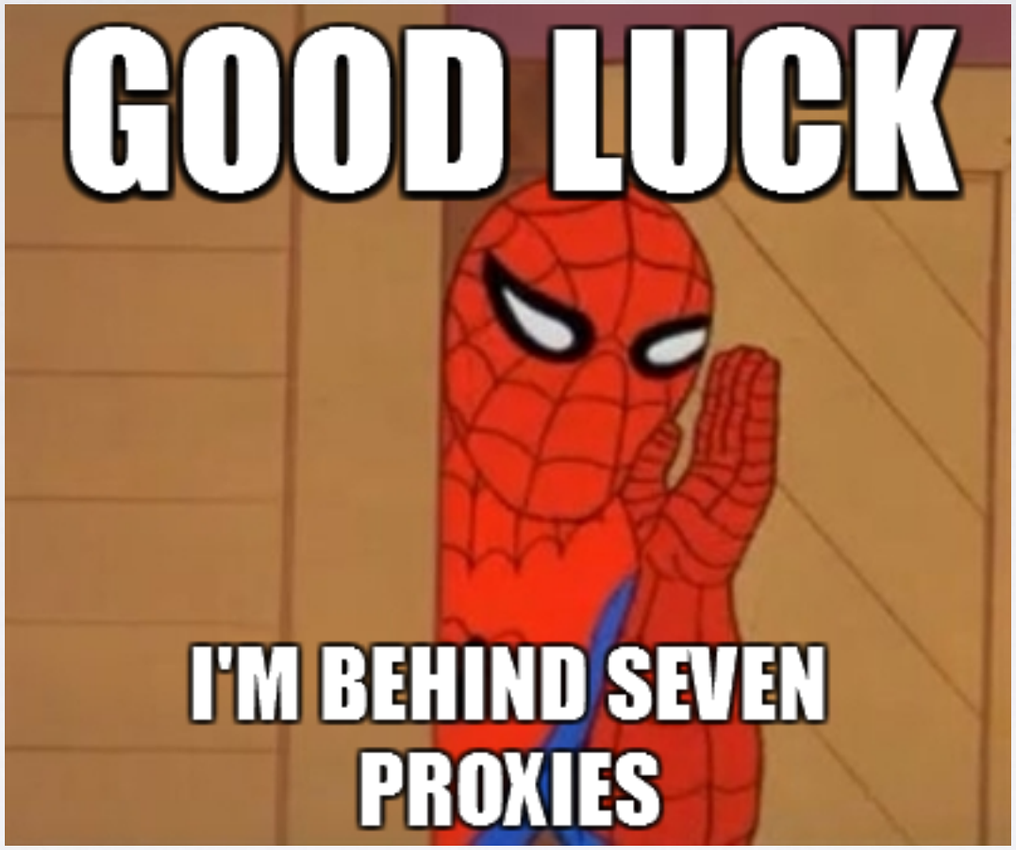


TECHNOLOGICALLY
IMPAIRED HACKER
wears a mask because he can't figure out how to put tape over the webcam

AUG
VIRGINIA
14
ZZZZZZZ

I'VE KILLED BEFORE AN' I'LL KILL AGAIN! I WON'T SPLIT THAT DOUGH WITH NO ONE -- NOT EVEN MYSELF!

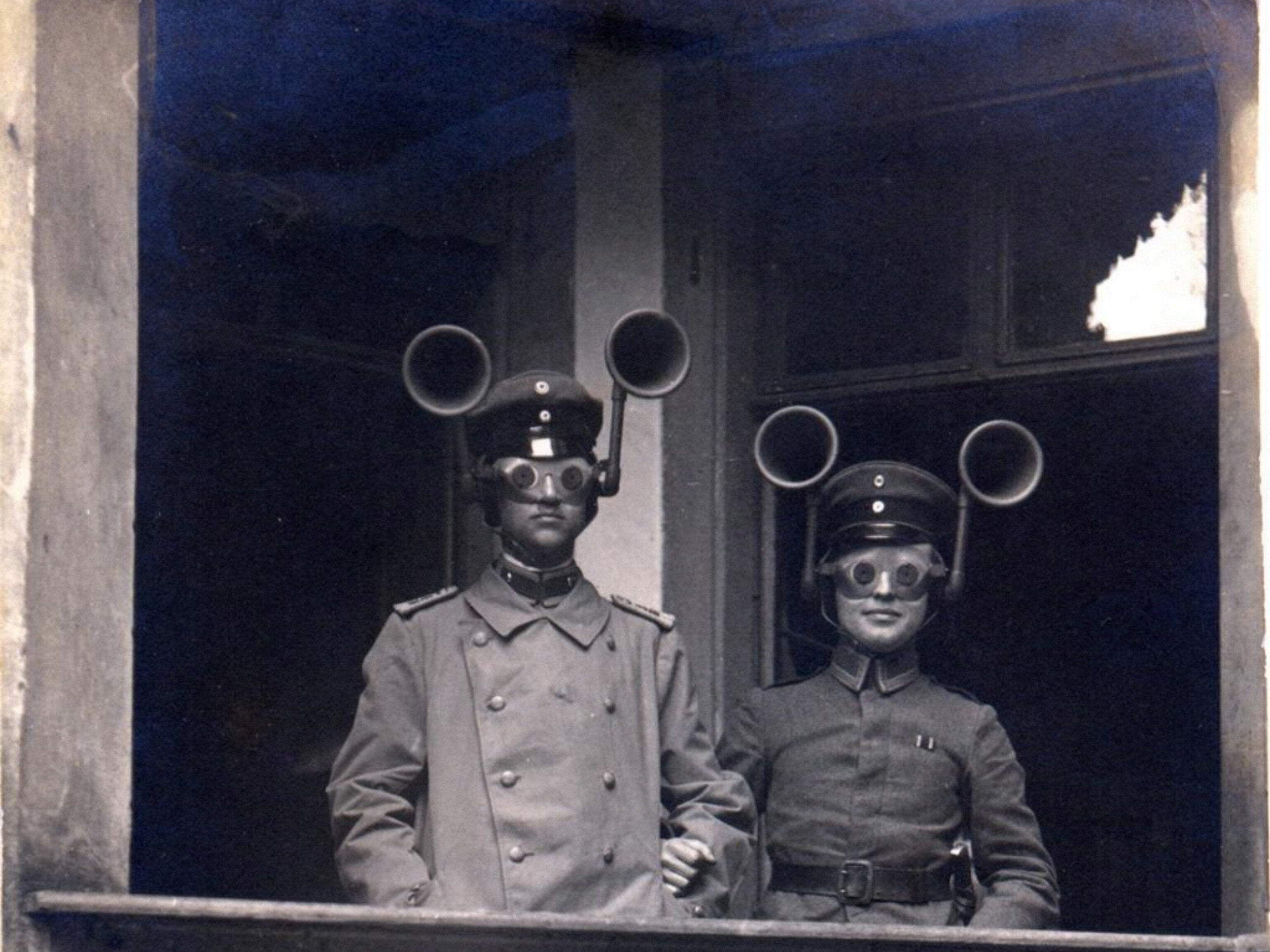
AXEL
x3
TIME
99
PRESS 2UP START
ONLY TRUST YOUR FISTS
POLICE WILL NEVER HELP YOU
POLICE
CLAP


GOOD LUCK
I'M BEHIND SEVEN PROXIES

THE PERSONAL

internet address & password logbook

Keep favorite website addresses, usernames, and passwords in one easy, convenient place!

PETER PAUPER PRESS

TENNIS
TENNIS