less a talk than a bundle of vignettes on how “cyber” is done.

post cyberwar apocalyptic wasteland!
actually, I am talking about the real cyberwar that is happening right now, all the time. with nation state sponsored hackers attacking targets of national interest, i.e. everyone interesting.
too many talks about bullshit theoretical crap “what if cyber pompeii”, or down in the weeds “how Unit 61398 does this”… not nearly enough on why or why it works.


HACKERS STEAL BILLIONS OF INTERNET DATA
IPHONE 6
MCDONALDS FAST LUNCH
GLUTEN FREE F
HEADLINES: REPORT: CHILD HAS BEEN BITTEN BY A SHARK AT FOLLY BEACH

not this…

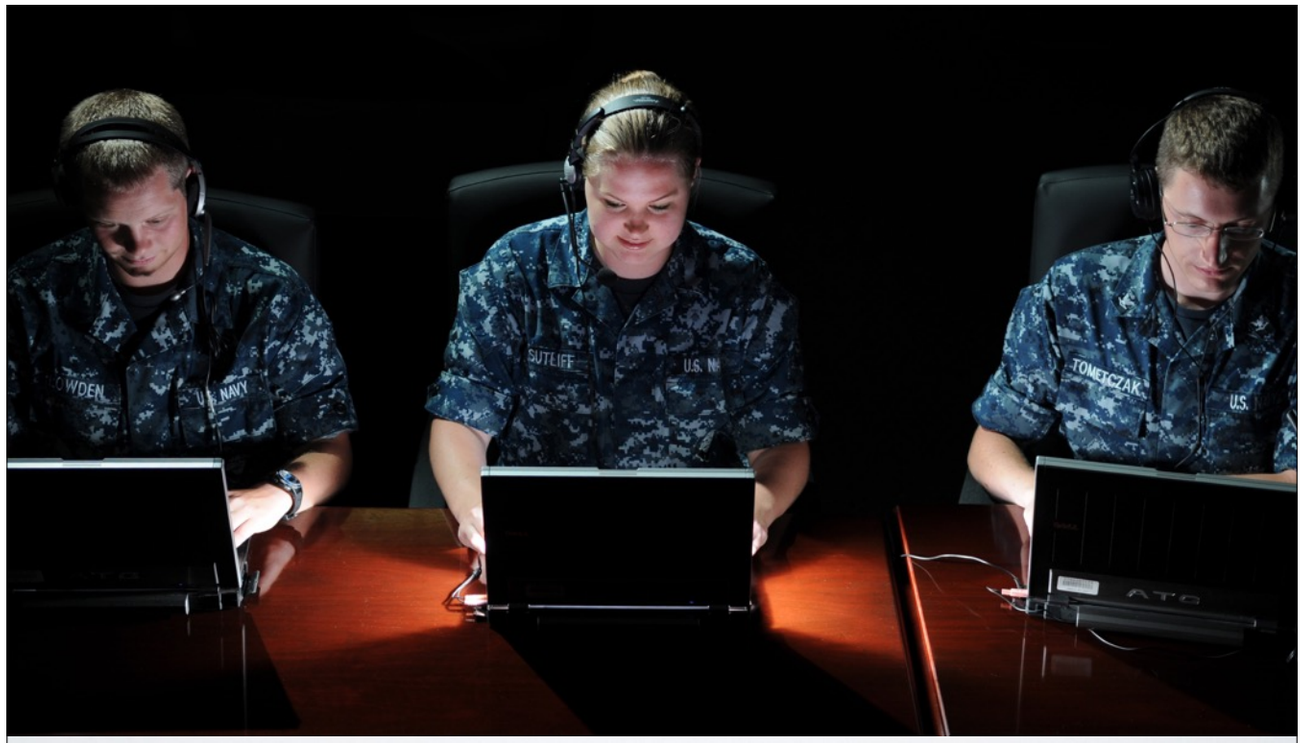
CYBERWAR

- ugh, I want to punch myself already
- Cyberwar is happening right now
  - Espionage
  - Seldom kinetic

the only kinetic stuff we know about for sure is stuxnet and Israel’s attacks against Lebanese anti-aircraft systems.

CYBER WAR

we thought we knew what to expect with cyberwar. awesome highly skilled people being individual awesome heroes through their individual prowess. Just like hackers on IRC, only more of them and more fun targets! w000000



WELL, THATS DISAPPOINTING

all the excitement of sitting around in front of a computer for hours plus the thrill of being a small cog in a large machine. Joy.

HOW WERE WE SO WRONG?

why is our cyberwar so crappy compared to the one we were promised?

NEW DOMAINS OF CONFLICT

…ARE INFREQUENT

…REALLY HARD TO PREDICT

THEORY, MEET PRAXIS

THIS HAS HAPPENED BEFORE.

AN ANALOGY

but first an analogy… all analogies are wrong, but some analogies are useful (to misappropriate a phrase)

A COMPLETELY NEW DOMAIN IN WARFARE

when else have humans invented a new domain in warfare that they had to develop and explore while engaged in combat?

AIR WAR 1915

an entirely new domain in warfare which nothing beforehand could prepare people for
* how to exploit it
* how to fight in it
what would be deciding factors in winning?
tactics invented form scratch.

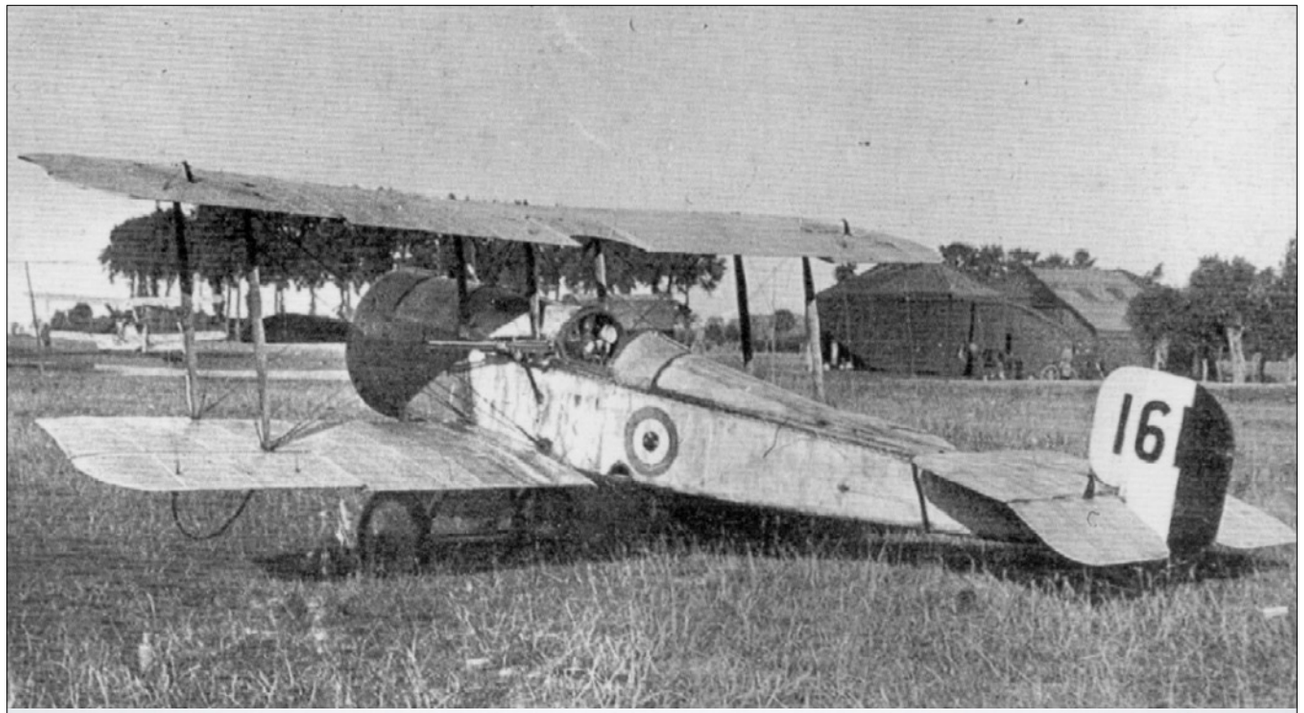
AIR WAR 1915

- Early planes were basically motorised kites
- No weapons
- Used for reconnaissance
  - So important that "*without it, artillery is blind*"

AIR WAR THEORY 1915

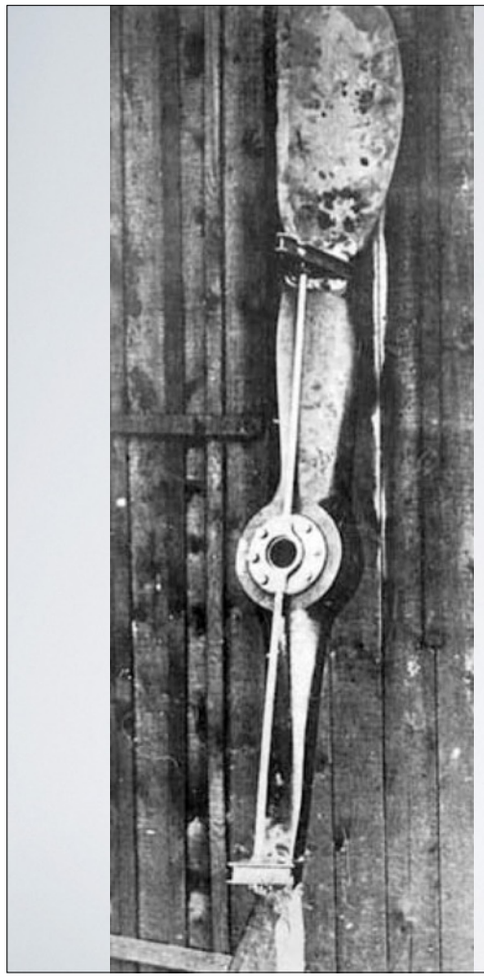
- Highly skilled pilots
  - In highly manoeuvrable planes
  - Battle for supremacy in bouts of skill and daring!
- Takeaway
  - Build highly manoeuvrable planes

START PRACTICING



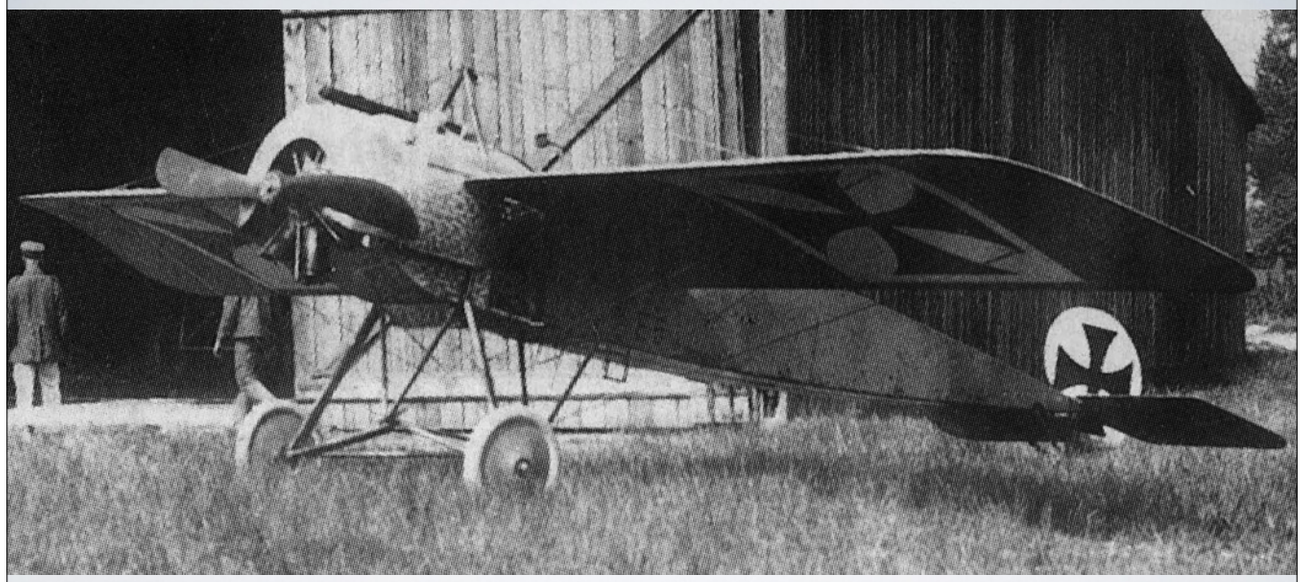
EARLY HACK JOB

the difficulty with mounting a gun on a plane is to avoid the propellor arc (otherwise you crash and die). very first hack was to just mount the gun at an angle on the side. Bristol Scout C, flown by Lanoe Hawker, july 15 1915 shot down 3 German planes



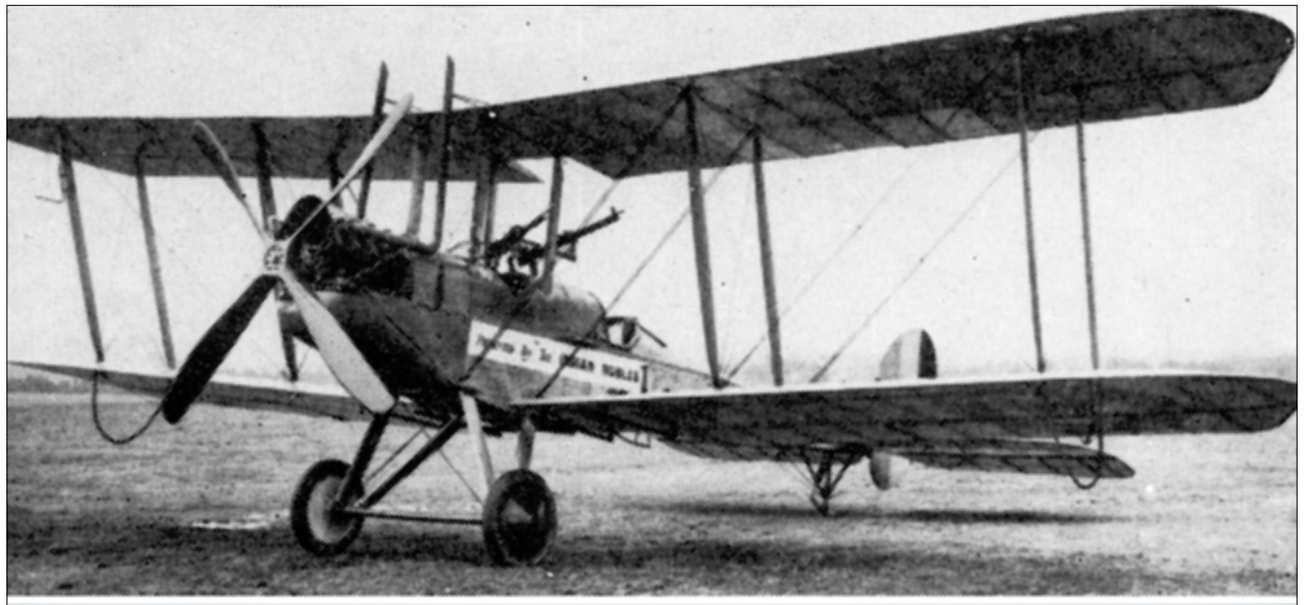
FIRST SUCCESSFUL HACK JOB

deflectors mounted on the propellor blade to send bullets ricocheting off to the side. Enabled the first “air ace”, Ronald Garros, shooting down four planes, but damaged the crank shaft and caused the plane to crash behind German lines. Oops.



FIRST MVP
THE FOKKER SCOURGE

the first synchronised machine gun was in the Fokker M5K. It had terrible performance characteristics, really abysmal. But it had a forward facing gun. No one else could hit anything, so the Fokker reigned supreme. Germans had air superiority.



THERE ARE TWO TYPES OF PLANES: FIGHTERS, AND TARGETS.

this is a target. Too slow, and with no credible air defence capability, the Fokkers chewed them up.

PRACTICAL RULES FOR AIR WAR

after a few years

DICTA BOELKE

- Secure the upper hand before attacking
- Always continue an attack you have begun
- Only fire at close range, when target is in sights
- Always keep an eye on your opponent

DICTA BOELKE CONT.

- In any attack, attack from behind
- If opponent dives on you, turn to meet the attack
- When over enemy lines, never forget line of retreat
- Attack in groups

eventually it reached a local maxima of perfection. a set of tactics (the dicta), along with aircraft that were functional enough to work, and sufficiently skilled operators to implement the tactics properly.
NOTE: airplanes have only offence capabilities, like cyber.

GO IN QUICKLY

PUNCH HARD

GET OUT

AIR WAR PRAXIS 1918

- Go in high and fast
- Surprise an unsuspecting enemy
- Gang up on weak targets
- Takeaway
  - Fast, high climbing planes. Lots of them.

CYBERWAR 2015

after years of hacking shit for realz, what have the professionals actually learned?

CYBERWAR THEORY 2000

CYBER TACTICS

go in like a fucking freight train

QUANTUM

- Why does NSA hit browsers?
  - Targeted
  - Easy*
  - It works

APT

- Why does Asia Pacific Threat do spear phishing?
  - Targeted
  - Easy
  - It works

WHAT WORKS

- Client sides
  - Spear phishing
  - Browsers
- USB
- Web Apps
- Other:
  - Interdiction, telnet sniffing, big boy stuff…

OVERWHELM THE WEAK

go after the weakest targets (client sides [optionally: against non security staff computers])

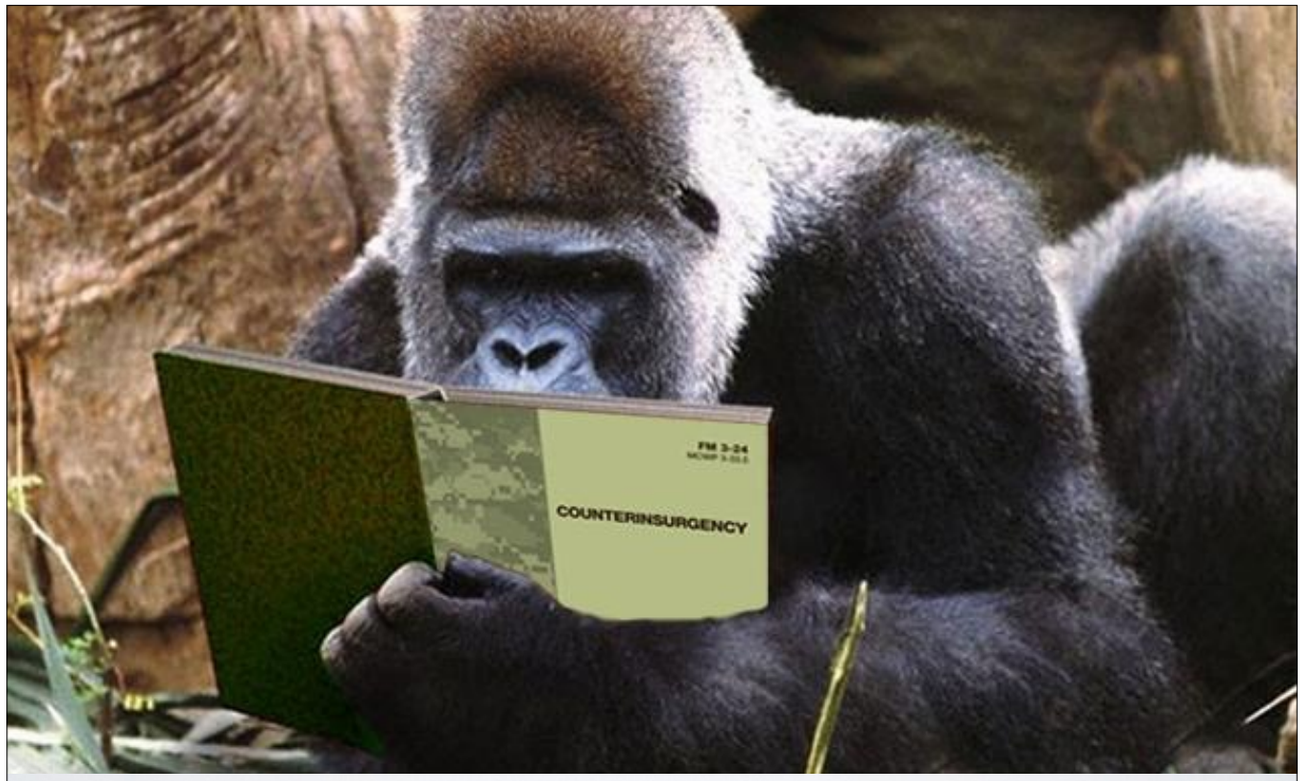
GO IN QUICKLY

PUNCH HARD

GET OUT

NEW CONFLICT DOMAIN

- Tactics invented in the crucible
- Early theory is probably wrong
  - Need praxis for validity
- What works isn't always what's elegant
  - "If it's stupid but it works, it's not stupid"



SPEC OPS

Theory and Practice

special operations theory describes the hacker process really well. spec ops theory describes how a small force is able to conduct operations against a larger force, and complete their mission successfully.

OPERATION PHASES

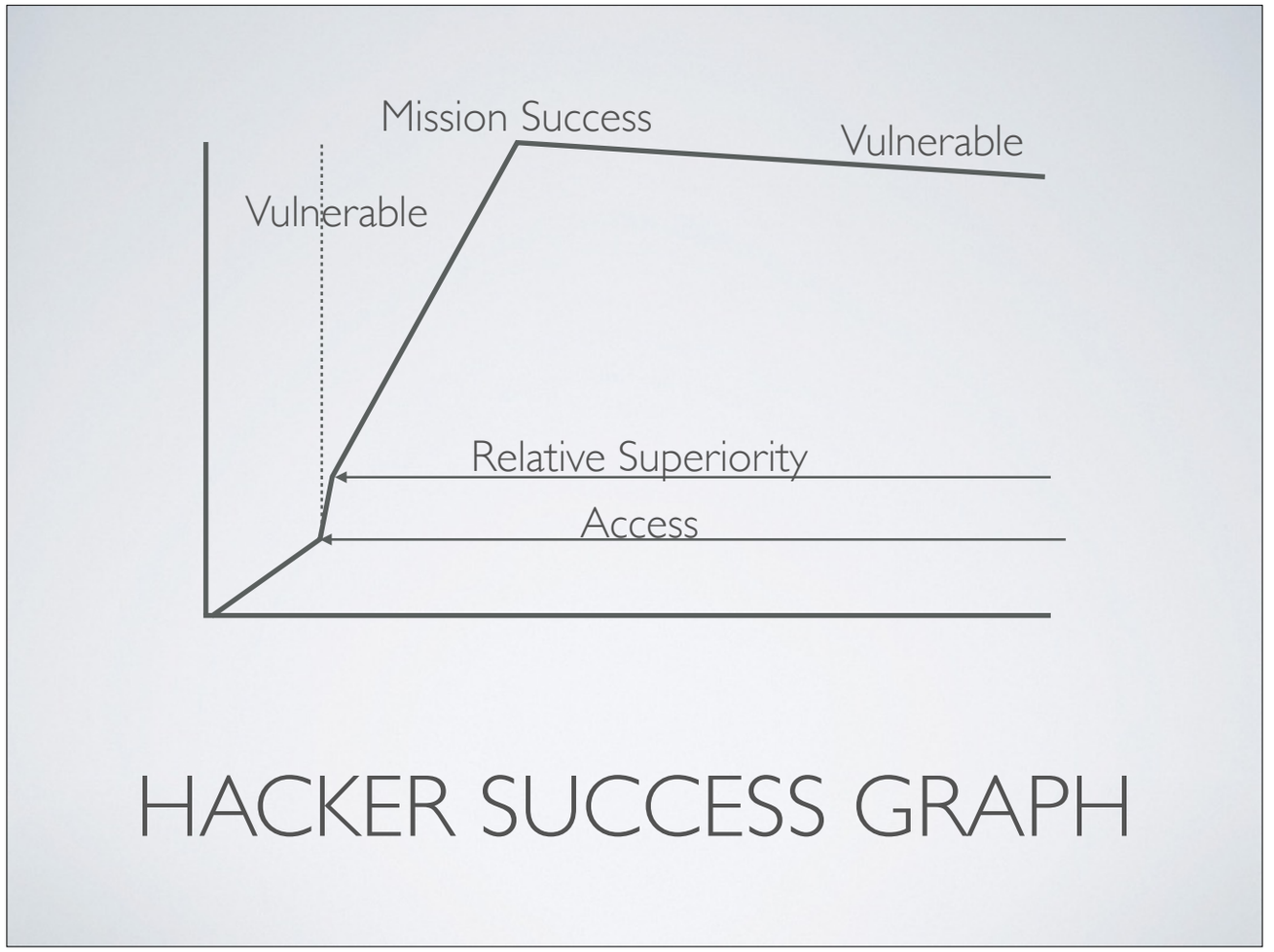
- planning
- preparation
- execution

very basic highlights of the phases that an operation goes through.

SPEC OPS

- simplicity
- security
- repetition
- surprise
- speed
- purpose

no one buys an exploit, they buy a capability. something that allows them to achieve their purpose.



a typical APT style hack. gain access to a device, elevate privileges, lateral traversal. mission success, then a long period of exposure while exfiltrating and retaining persistence

- point of vulnerability
  - (initial contact)
- relative superiority
  - (overwhelm local defences)
- mission completion
- area of vulnerability
  - function of time it takes to achieve mission completion

ADVERSARIAL ORGANISATIONS

organisations are organisations.
they have bosses, budgets, missions, constraints. they are just like other organisations.

how to pick which one hit you?

CHINESE HACKERS

RUSSIAN HACKERS

INDIAN HACKERS

LAME HACKERS

TOOLCHAINS

- An investment and an expense
  - Constant maintenance
- Tools, Techniques & Procedures are Commitments

toolchain maintenance and development. once you commit, you're committed. changing is expensive.
developing a new toolchain is expensive, but then add in retraining costs…

if you train 500 guys on how to develop, send and exploit spear phishing attacks, switching to browsers has a cost.
lower productivity, lower performance, retool costs, retraining costs, etc. etc.
less efficiency and lower productivity is a serious problem.

INFOSUCK INDUSTRY

while the professionals are making a living cybering the world, what is the infosec industry doing?

security conferences have really amazing stunt hacking. sometimes spectacular stuff, sometimes “look at this debug port debugging”
the industry is stunt hacking with selfie sticks while the internet burns

meanwhile, the actual job is left to less glamorous roles doing dirty jobs…

“the long walk” — IRA bomb

the cool thing about this cyberwar is that it is a lot like disaster journalism by tourists… you got all of the infosec industry taking selfies (blog posts + hot takes) while everything burns.
“lol, read my hot take on Target and buy my service”

security vendors. don’t actually deliver what they promise.

CISSP

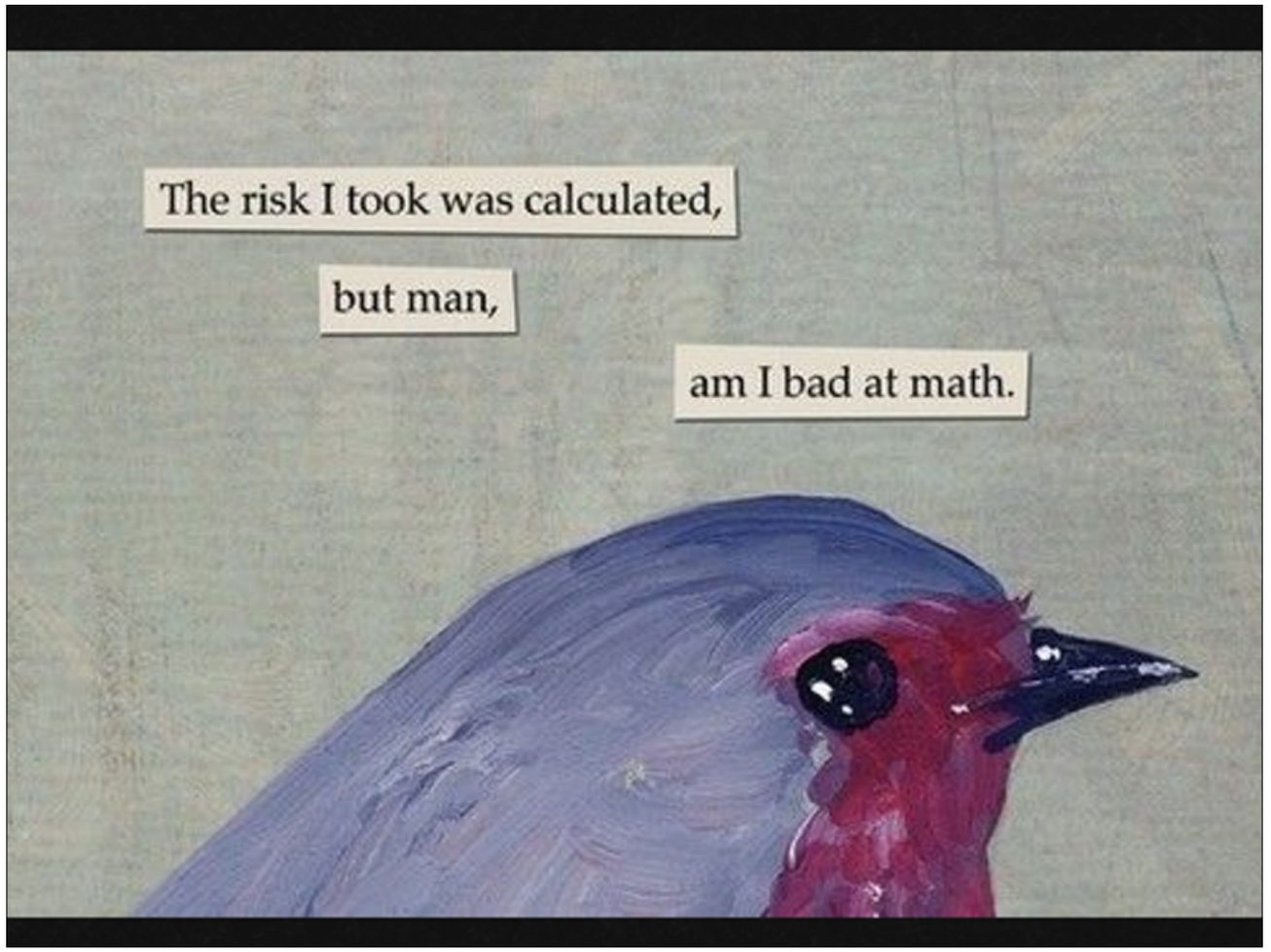
securing your critical infrastructure with CISSPs? Good luck with that…

this is what a malware looks like, we saw one once.
new AV based on “this is what they looked like last time we found one”…

PLOT TWIST — it was Iran!

because real offensive teams don’t need to be the best, they only need relative superiority until they achieve mission success
“lol, chinese APT is weak sauce. how does it ever work?” — relative superiority. 0lday vs CFO laptop == pay day.

good news though, i guess… even the best don’t always win.


The risk I took was calculated,
but man,
am I bad at math.


FIN

CONCLUSION

- Tactics forged in the crucible
  - hit the weakest the hardest
- Relative Superiority + Purpose = Success


HACK THE PLANET!