i’m going to talk about the game, how the game change, strategies and tactics for the game.

I’ve been in cyber security industry since 1998/99.
Some of you have too. Some of you are just starting. I’ve seen the changes that have come down the road when I started, cyber was fun.

something like this…

the game used to be fun. hack boxes at night, code during the day, wait to get a job somewhere

THE GAME

a corporate job / CERT / AV or hug security / security research
predictable; deal with vulnerable software, deal with securing a network against opportunists or low skill criminals trying to make some money

THE GAME: CYBERSECURITY 2000

- Cleanup after breaches
  - Usually by script kiddies w/ egg drops
- Clean up malware
  - Sometimes by cybercriminals
- Coordinate vulnerability disclosure
  - (At least this one has been solved)

the actual job was pretty exciting and challenging.
Everyone was cleaning up after script kiddies, cleaning up malware, coordinating vuln disclosures (thank god thats solved)
cleanup breaches, cleanup malware, cleanup vuln code; basically internet janitor.

THEN, ONE DAY...

THE GAME GOT WEIRD

then one day the job got weird. this was about 2010 plus or minus a year or so (def by 2011, stuxnet script kiddies, viruses, cybercriminals, … KGB? PLA? NSA? WTF?

the great game is the global espionage business that all nation states engage in to one degree or another.

THE GREAT GAME

APT

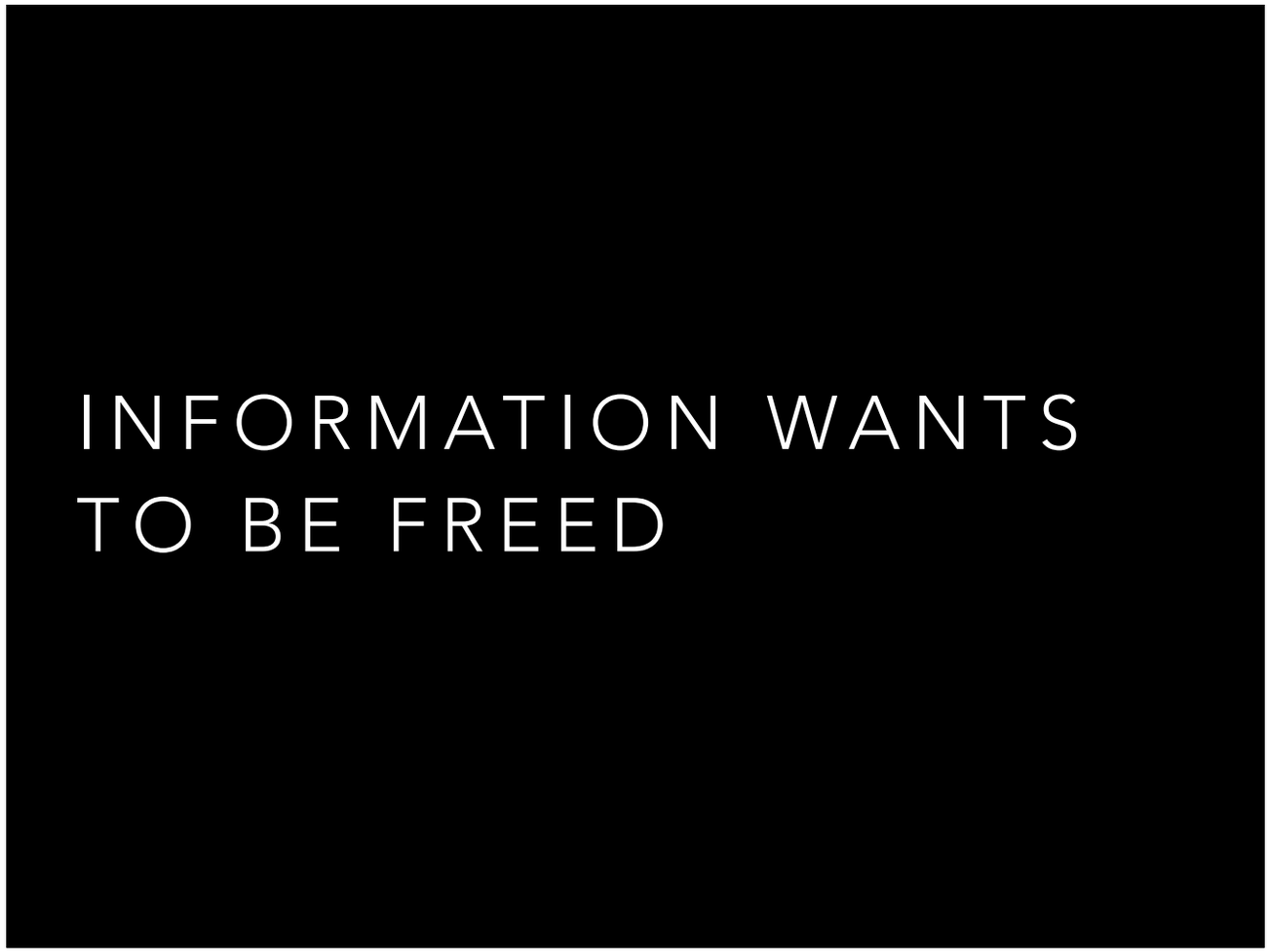
more accurately, the Great Game (espionage) that had always been happening was suddenly now also happening online. in cyber.
the Asia Pacific Threat got sufficiently capable to operationalise cyber espionage
(Shanghai Jiao Tong University)

the russians were early to the game (see the Cuckoo’s Egg, over 20yrs old)
They are extremely capable now, huge resources to draw on from their unchecked cybercriminal citizenry

massive investment in tools and technology, plus decades of experience. See “the Morris worm, 1988”
“SIGINT at rest” stolen from CIA

INEVITABLE

the merging of cybersecurity and espionage was inevitable.
espionage is about collecting information, all the information is on computers



spies collect data. data is on computers. spies collect from computers. QED
this is how it always has been… remember: morris worm 1988, cuckoos egg 1989. “they haven’t gone away you know”
our world has collided with their’s, which means

all the stuff that used to matter still matters: malware, vulnerabilities, criminals, kiddies
but we share the space with nation states
we’re players in the great game; particularly the people that are doing APT research, they’re active players in the intelligence space and making their decisions in the marketing dept!


WE’RE HERE

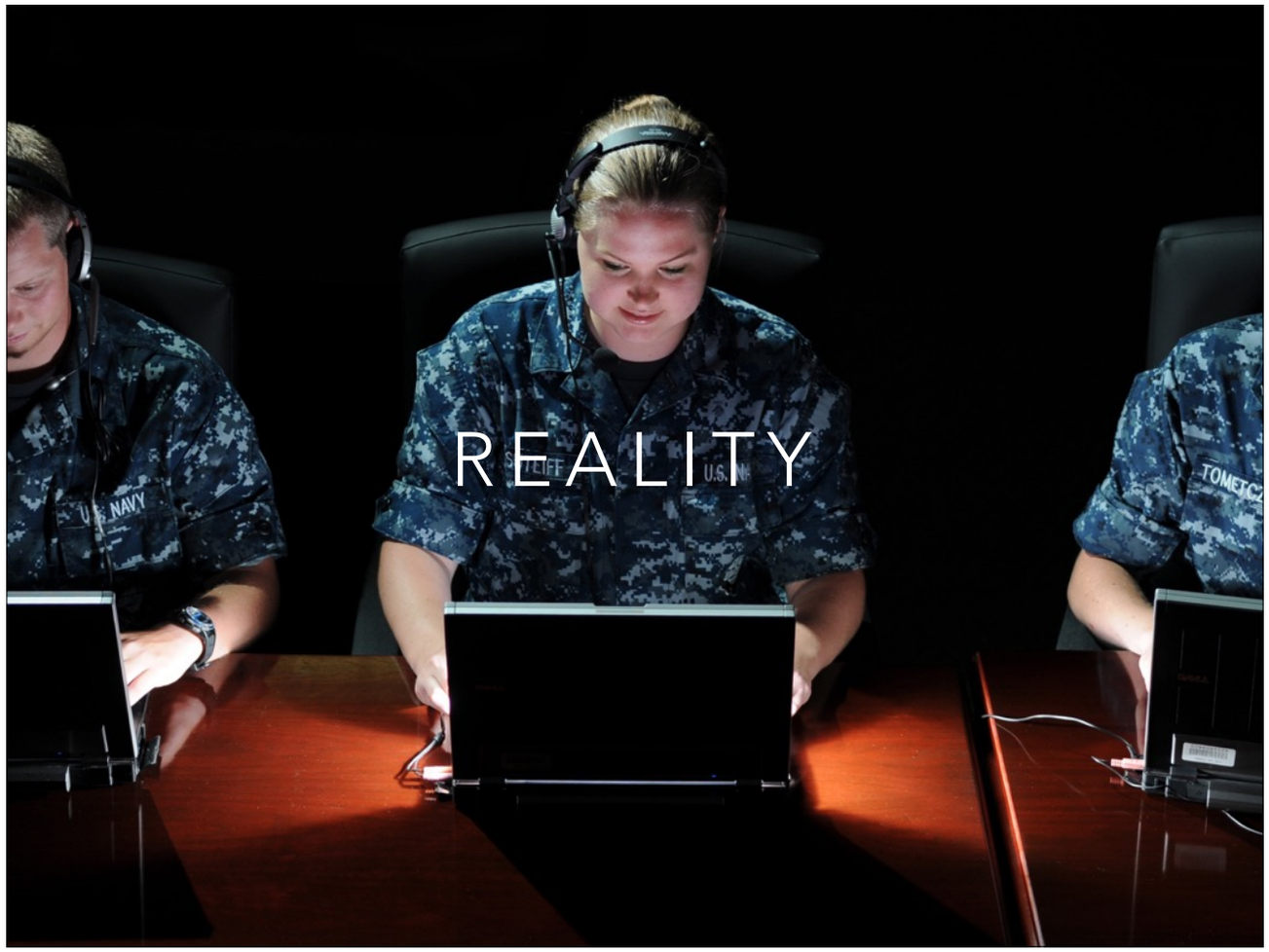
NOW WHAT?

we’re living in a global espionage free for all where everyone is a potential target
how do we live with this?
watching the emergence of a new strategy and

THE GREAT CYBER GAME

cyberwar is not a thing that is happening.
there is global free for all cyber espionage, and cyber conflict, and cyber crime, but it isn’t war.
it is more interesting than that…

smart single skilled hackers would battle it out in a game of wits
the most highly skilled hacker with the most knowledge would “win”, would be heroes



reality sucks.


WELL THAT SUCKS

WHY SO VERY WRONG?

everyone seems to have gotten cyber wrong. this is because the theory was developed by people who had no experience (no one had experience)

NEW DOMAINS OF CONFLICT

ARE INFREQUENT

there have been 3 in the last 100 years (which is more than in the last 100,000 years)
domains: land, sea, air, space, cyber
space hasn’t had open conflict, so a lot is still theory. just air and cyber are active, “hot” domains

HARD TO PREDICT

THEORY MEETS PRAXIS

THIS HAS HAPPENED
BEFORE

AN ANALOGY

all analogies are wrong, but some analogies are useful…

A NEW DOMAIN OF CONFLICT

the last time humans created a new domain of conflict and then evolved the theory tactics and strategy while engaged in active conflict


AIR POWER 1915

AIR POWER 1915: TECHNOLOGY

- Airplanes were basically motorised kites
- No weapons
- Used for reconnaissance
  - Critical to accurate artillery fire

“without [airplanes], artillery is blind”

AIR POWER: TACTICAL THEORY

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

PRACTICE...

AIR POWER 1917: EXPERIENCE

- Practical rules for air war
  - Boelke Dicta
  - Similar rules from Western aces
- Proven in the crucible
- Concerned only with winning, not chivalry
- Takeaway
  - Fast planes that can climb high

turns out the only thing that actually matters in a dog fight is who starts out higher up and who can get in and out fastest.

DICTA BOELKE

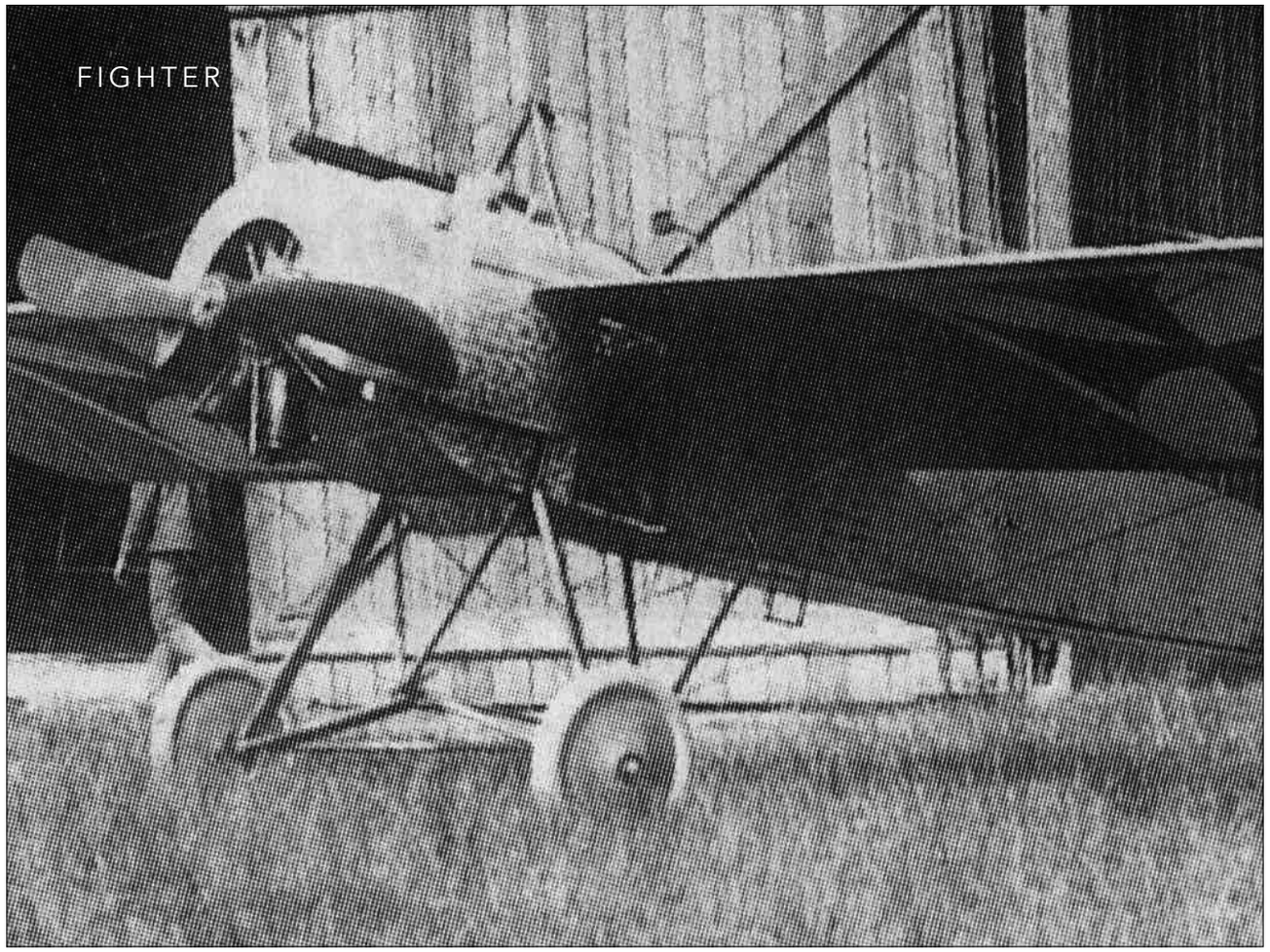
- Secure the upper hand before attacking
- Always continue an attack you have begun
- Only fire at close range, when target is in sights
- Always keep an eye on your opponent

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

"There are two types of planes: fighters, and targets"

AIR FORCE SAYING



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.


TARGET

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.

OVERWHELM THE WEAK

GO IN QUICK

HIT HARD

GET OUT


TACTICAL CYBER

really awesome skilled individuals battling it out in bouts of extreme skill
actual operators are less skilled than the toolchain developers (usually). the real skill is in the tool development stage

CYBER CONFLICT 2015: PRACTICE

- Experience has produced some basic rules about winning
  - Hit the softest targets the hardest

this is about achieving mission objectives, not scoring cool points
success is the the only criteria that matters

TARGETED ATTACK DEMO

QUANTUM

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

NSA is privileged in how much traffic they have access to. Other nation states don’t have such access, they need to “go to the mountain, because the mountain doesn’t come to Mohamed”
There are Quantum boxes for a single nation (e.g. Iran, etc) but not Internet scale.

APT

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

EVERYONE

- Why do all* nation states use phishing?
  - Targeted
  - Easy
  - It works

phishing is built on existing national intelligence agency competencies: recruiting people is what they do (assessment and recruitment are core espionage skills)
if you can persuade someone to betray their country, persuading them to click a link is easy
hard to detect and block, never gets patched.
obfuscated malware installers

WHAT WORKS

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

80/20… client sides for everyone, then other more obscure stuff for hard targets
USB for air gapped networks (usually)
web apps mostly only to then use that web app for launching browser attacks
interdiction, etc are the long tail of cyber…

go in like a fucking freight train

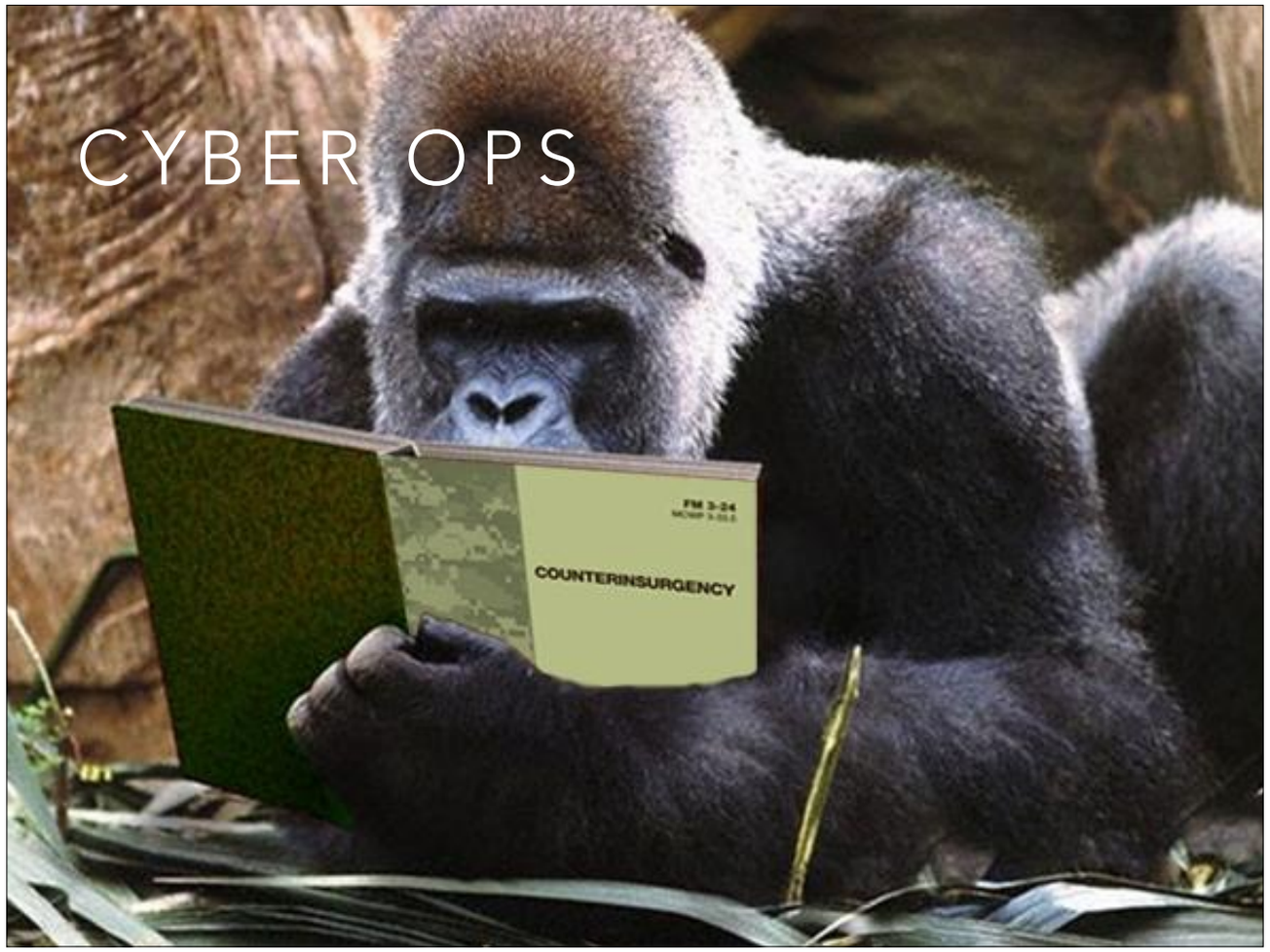
OVERWHELM THE WEAK

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

GO IN QUICKLY

HIT HARD

GET OUT


CYBER OPS
FM 3-24
COUNTERINSURGENCY

OPERATION PHASES

- planning
- preparation
- execution
- finish

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.

it looks like this.
notice he’s using kali.

ADVERSARIAL ORGANISATIONS

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


CHINA


RUSSIA

INDIA


"Non-Violence is the greatest force at the disposal of Mankind.
It is the supreme law. By it alone can mankind be saved."
-Mahatma Gandhi
MOHANDAS K. GANDHI
October 2, 1869 - January 30, 1948
"My Life is My Message"


NORTH KOREA
Belnea
FUJITSU SIEMENS

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.

STRATEGIC CYBER

"data packets are like bullets and your walls of fire are like the armor that repels them."

–TWO STAR GENERAL, CYBER COMMAND

http://malwarejake.blogspot.kr/2015/10/were-making-our-military-leaders-stupid.html

THE TECHNICAL MEANS OF WARFARE

AERONAUTICS OPENED up to men a new field of action, the field of the air. In so doing it of necessity created a new battlefield; for wherever two men meet, conflict is inevitable. In actual fact, aeronautics was widely employed in warfare long before any civilian use was made of it.[7] Still in its infancy at the outbreak of the World War, this new science received then a powerful impetus to military development.

The practical use of the air arm was at first only vaguely understood. This new arm had sprung suddenly into the field of war; and its characteristics, radically different from those of any other arm employed up to that time, were still undefined. Very few possibilities of this new instrument of war were recognized when it first appeared. Many people took the extreme position that it was impossible to fight in the air; others admitted only that it might prove a useful auxiliary to already existing means of war.

we don’t really know what strategic cyber means… there has been stuxnet, there has been espionage, but what is strategic?
replace “air” with “cyber” on this page, and you have the best overview of emerging cyber strategy…

WHAT CAN HELP?

how do you stop a targetted attack by a nation state?

your job kinda sucks now

“the long walk” — IRA bomb

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

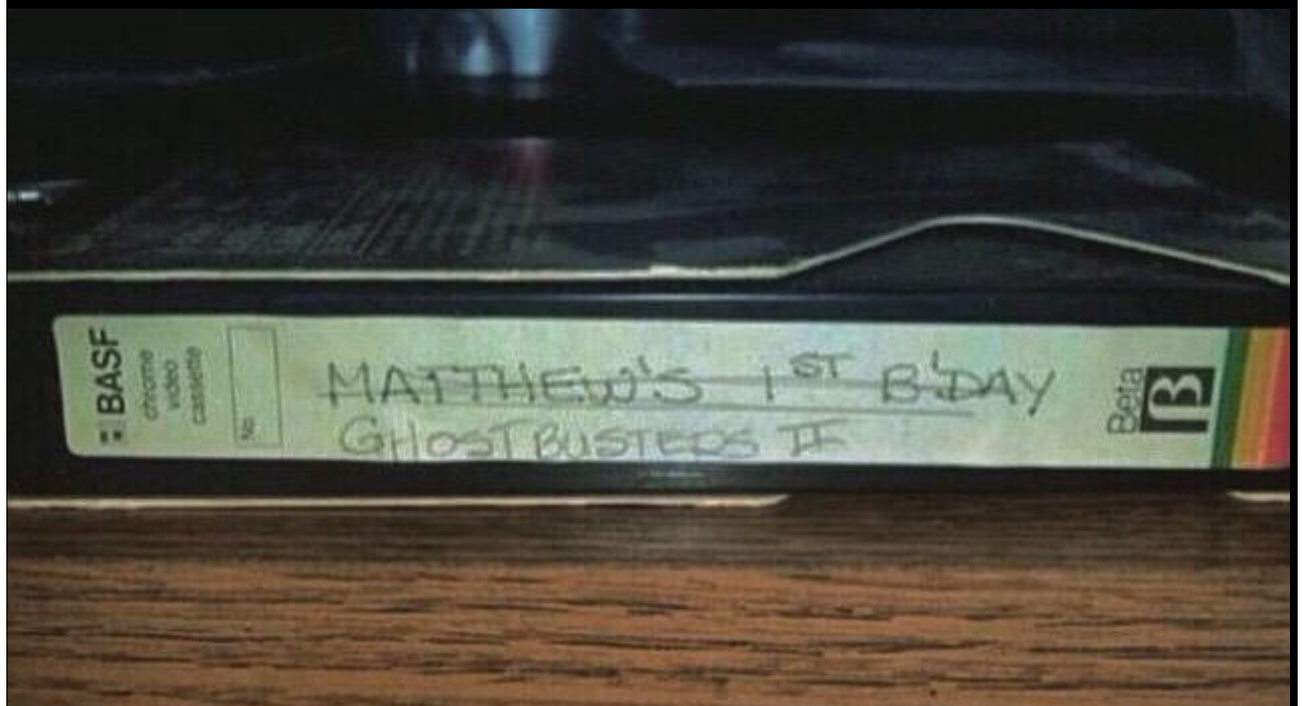
security conferences have really amazing stunt hacking. sometimes spectacular stuff, sometimes “look at this debug port debugging”
the industry is stunt hacking with selfie sticks while the internet burns

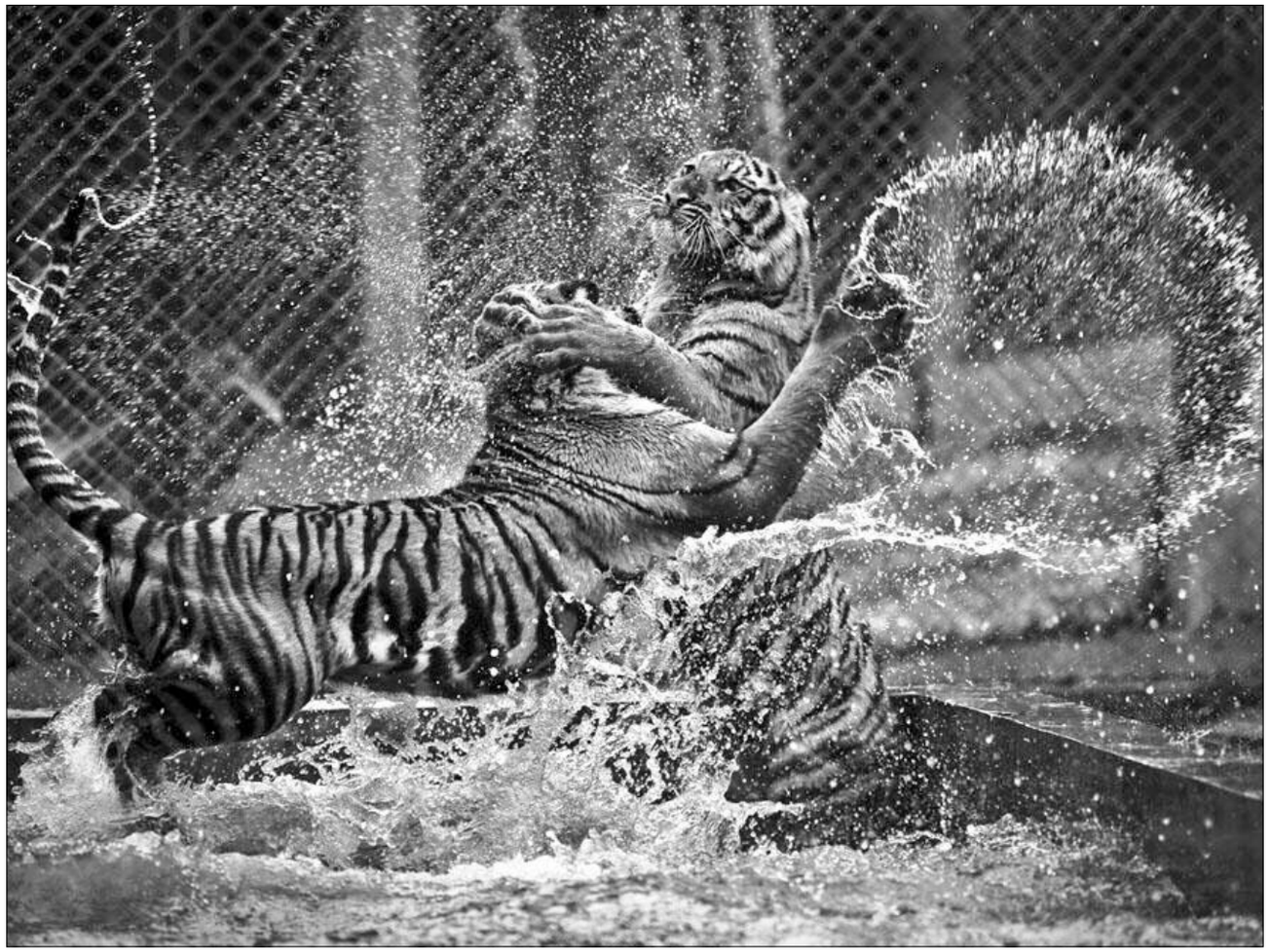
the cool thing about this cyberwar is that it is a lot like disaster journalism by tourists… you got all of the infosec industry taking selfies (blog posts + hot takes) while everything burns.
“lol, read my hot take on Target and buy my service”

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

NATIONAL INTELLIGENCE AGENCIES

DON'T LOVE YOU





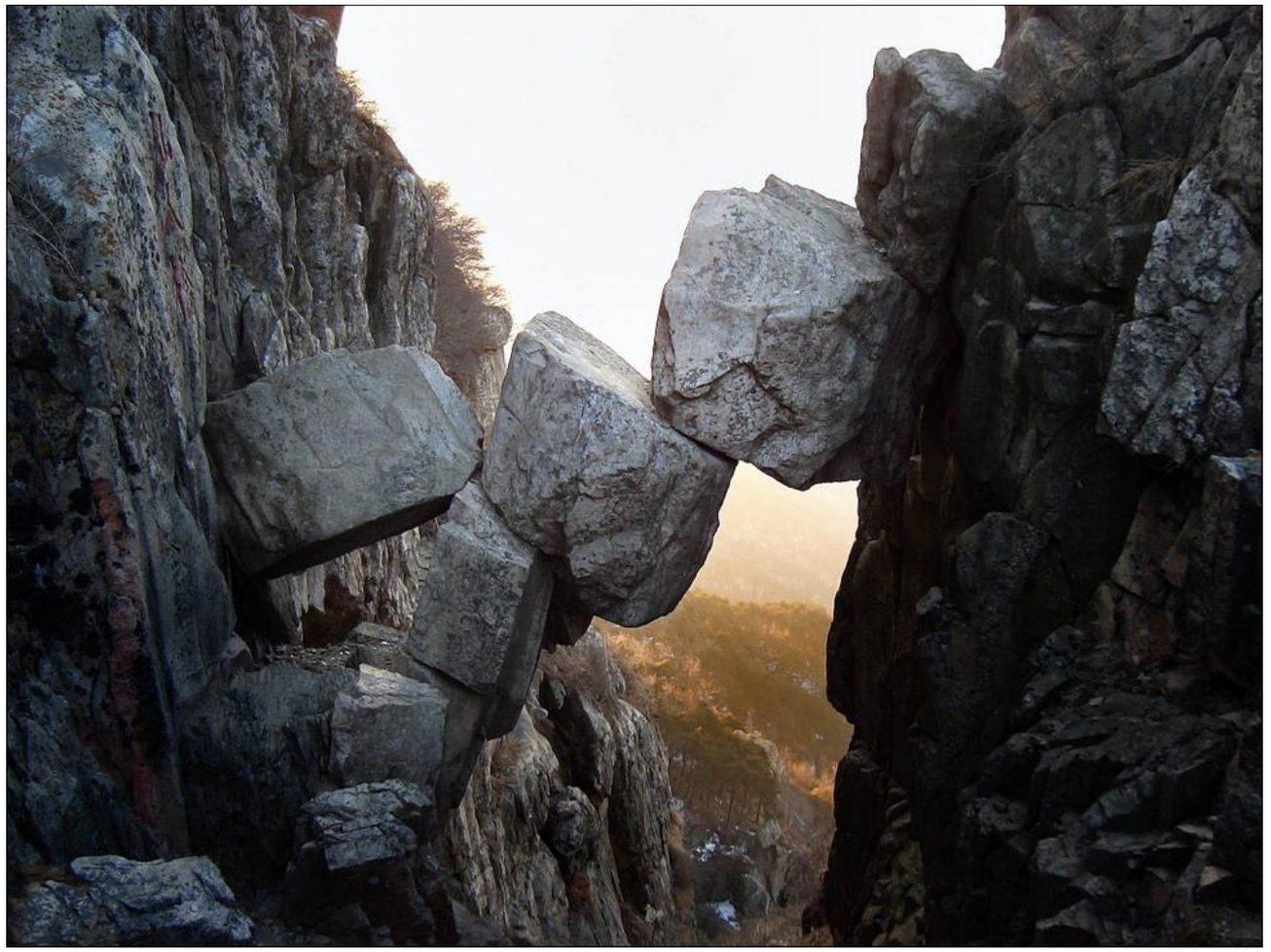
they have more important things to do anyway, contest other national intelligence agencies

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”…

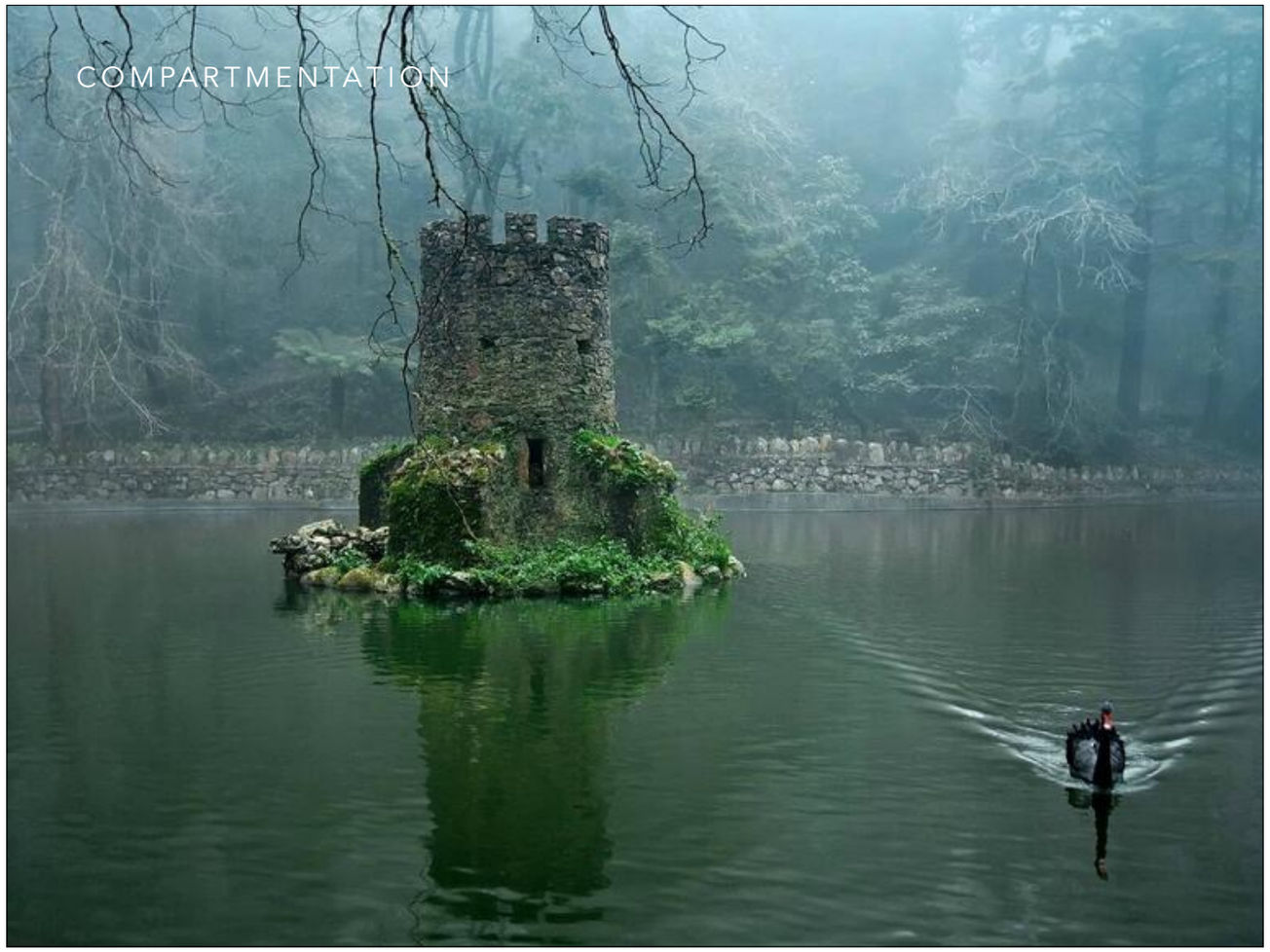
WHAT WORKS

early detection
extreme examples of this are available from some vendors, i won’t name: instrument the enterprise, e.g. el Jefe

ideal network architecture. known ingress egress points. self contained.



but it looks like this



impact containment

a lesson from bank vaults
you can’t stop a bank robber (man with a gun does what he wants)
so you make it resource expensive w/ the only resource that is scarce, time
this isn’t how you stop bank robberies (not exactly)

this. it is impossible to access any serious number of locked boxes inside of 2 minutes.

good news is, with all that, you might just catch… the A team.

but anyway, this is an exciting time to be alive.

THANK YOU